Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR05/000615

International filing date: 04 March 2005 (04.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2004-0098527
Filing date: 29 November 2004 (29.11.2004)

Date of receipt at the International Bureau: 17 May 2005 (17.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

대한민국 특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office

출 원 번 호 : 특허출원 2004년 제 0098527 호
Application Number 10-2004-0098527

출 원 일 자 : 2004년 11월 29일
Date of Application NOV 29, 2004

출 원 인 : 한국전자통신연구원 외 5 명
Applicant(s) Electronics and Telecommunications Research Institute, et al

2005 년 04 월 07 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2004.11.29

【발명의 국문명칭】 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법 및 그 프로토콜 구성 방법, 그리고 가입자 단말에서의 트래픽 암호화 키 상태 머신의 동작 방법

【발명의 영문명칭】 METHOD FOR MANAGING TRAFFIC ENCRYPTION KEY IN WIRELESS PORTABLE INTERNET SYSTEM AND PROTOCOL CONFIGURATION METHOD THEREOF, AND OPERATION METHOD OF TRAFFIC ENCRYPTION KEY STATE MACHINE IN SUBSCRIBER STATION

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【출원인】

【명칭】 삼성전자 주식회사

【출원인코드】 1-1998-104271-3

【출원인】

【명칭】 주식회사 케이티

【출원인코드】 2-1998-005456-3

【출원인】

【명칭】 주식회사 케이티프리텔

【출원인코드】 1-1998-098986-8

【출원인】

【명칭】 에스케이텔레콤 주식회사

【출원인코드】 1-1998-004296-6

【출원인】

【명칭】 하나로통신 주식회사

【출원인코드】 1-1998-112749-2

【대리인】

【명칭】 유미특허법인

【대리인코드】 9-2001-100003-6

【지정된변리사】 이원일

【포괄위임등록번호】 2001-038431-4

【포괄위임등록번호】 2002-036528-9

【포괄위임등록번호】 2003-082444-7

【포괄위임등록번호】 2002-031524-6

【포괄위임등록번호】 2002-062290-2

【포괄위임등록번호】 2004-014783-3

【발명자】

【성명의 국문표기】 조석헌

【성명의 영문표기】 CHO,SEOK HEON

【주민등록번호】 770127-1543416

【우편번호】 570-976

【주소】 전라북도 익산시 신동 775-21번지

【국적】 KR

【우선권 주장】

【출원국명】 KR

【출원종류】 특허

【출원번호】 10-2004-0046756

【출원일자】 2004.06.22

【증명서류】 첨부

【우선권 주장】

【출원국명】 KR

【출원종류】 특허

【출원번호】 10-2004-0015162

【출원일자】 2004.03.05

【증명서류】 첨부

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 유미특허법인 (인)

【수수료】

【기본출원료】 0 면 38,000 원

【가산출원료】 96 면 0 원

【우선권주장료】 2 건 40,000 원

【심사청구료】 0 항 0 원

【합계】 78,000 원

【첨부서류】 1.우선권증명서류 원문[특허청기제출]_1통

【요약서】

【요약】

본 발명은 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키(TEK:Traffic Encryption Key) 관리 방법 및 그 프로토콜 구성 방법, 그리고 가입자 단말에서의 트래픽 암호화 키 상태 머신의 동작 방법에 관한 것이다. 이 트래픽 암호화 키 관리 방법은 멀티캐스트 또는 브로드캐스트 서비스용 트래픽 암호화 키를 기지국에서 자동으로 생성하여 가입자 단말에서 사용되는 트래픽 암호화 키를 주기적으로 갱신하는 방법으로, 기지국이 가입자 단말로 2종류의 키 갱신 명령 메시지를 송신하여 트래픽 암호화 키를 갱신한다. 이 때 2종류의 키 갱신 명령 메시지 중 제1 메시지는 트래픽 암호화 키를 암호화하는데 사용될 GKEK(Group Key Encryption Key)를 갱신하기 위한 것이고, 나머지 하나인 제2 메시지는 트래픽 암호화 키를 갱신하기 위한 것이다. 기지국은 가입자 단말에서 트래픽 암호화 키 갱신을 위해 설정된 시간(TEK Grace Time)과는 다른 시간(M&B TEK Grace Time)을 설정하여 관리하며, 이 설정된 시간 전에 GKEK를 갱신하기 위한 새로운 GKEK를 포함한 제1 메시지를 가입자 단말로 송신하고, 이 설정된 시간 후에 제1 메시지에 의해 송신된 새로운 GKEK로 암호화된 새로운 트래픽 암호화 키를 포함한 제2 메시지를 가입자 단말로 송신하여 가입자 단말에서 사용되는 트래픽 암호화 키를 갱신한다. 이 때, 제1 메시지는 프라이머리 매니지먼트 커넥션(Primary Management Connection)을 통해 가입자 단말로 각각 전송되고, 제2 메시지는 브로드캐스트 커넥션(Broadcast Connection)을 통해 가입자 단말 모두에게 동시에 전달된다. 본 발명에 따르면, 적은 신호 자원을

가지고도 트래픽 암호화 키의 갱신 및 분배가 가능하며, 또한 기지국 입장에서 이러한 트래픽 암호화 키와 관련된 처리량이 감소된다는 장점이 있다.

【대표도】

도 12

【색인어】

무선 휴대 인터넷, 트래픽 암호화 키, 키 갱신, 키 분배, 키 갱신 명령, TEK Grace Time, GKEK, MAC 메시지, PKM, privacy, IEEE 802.16

【명세서】

【발명의 명칭】

무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법 및 그 프로토콜 구성 방법, 그리고 가입자 단말에서의 트래픽 암호화 키 상태 머신의 동작 방법 {METHOD FOR MANAGING TRAFFIC ENCRYPTION KEY IN WIRELESS PORTABLE INTERNET SYSTEM AND PROTOCOL CONFIGURATION METHOD THEREOF, AND OPERATION METHOD OF TRAFFIC ENCRYPTION KEY STATE MACHINE IN SUBSCRIBER STATION}

【도면의 간단한 설명】

<1> 도 1은 본 발명이 적용되는 무선 휴대 인터넷 시스템의 개요를 도시한 개략도이다.

<2> 도 2는 도 1에 도시된 무선 휴대 인터넷 시스템의 계층 구조를 도시한 계층도이다.

<3> 도 3은 도 1에 도시된 무선 휴대 인터넷 시스템에서 기지국과 가입자 단말의 연결구조를 도시한 개략도이다.

<4> 도 4는 도 1에 도시된 무선 휴대 인터넷 시스템에서의 가입자 단말과 기지국 간의 연결 설정을 위한 흐름도이다.

<5> 도 5는 일반적인 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법의 흐름도이다.

<6> 도 6은 일반적인 무선 휴대 인터넷 시스템에서 복수의 가입자 단말과 기지국

간의 트래픽 암호화 키 갱신 방법의 흐름도이다.

<7> 도 7은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 갱신을 위한 암호 관련 PKM 파라미터 운용 범위를 나타낸 테이블을 도시한 도면이다.

<8> 도 8은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법의 흐름도이다.

<9> 도 9는 도 8에서 가입자 단말이 기지국이 갱신하여 브로드캐스트 커넥션을 통해 전송한 Key Reply 메시지를 올바르게 수신하지 못하였을 경우의 트래픽 암호화 키 관리 방법에 대한 흐름도이다.

<10> 도 10은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서 복수의 가입자 단말과 기지국 간의 트래픽 암호화 키 갱신 방법의 흐름도이다.

<11> 도 11은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에 따라 트래픽 암호화 키 분배시 MAC 헤더의 CID값과 이에 따른 트래픽 암호화 키를 암호화하는 입력 키간의 관계를 설명해 주는 테이블이다.

<12> 도 12는 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법의 흐름도이다.

<13> 도 13은 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서 복수의 가입자 단말과 기지국 간의 트래픽 암호화 키 갱신 방법의 흐름도이다.

<14> 도 14는 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래

픽 암호화 키 관리 방법에서 사용되는 트래픽 암호화 키 응답(Key Reply) 메시지의 내부 파라미터들을 나타낸 테이블을 도시한 도면이다.

<15> 도 15는 도 14에 도시된 트래픽 암호화 키 관련 파라미터(TEK-Parameters)를 을 표현한 테이블을 도시한 도면이다.

<16> 도 16은 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에서 사용되는 키 갱신 명령(Key Update Command) 메시지의 내부 파라미터들을 나타낸 테이블을 도시한 도면이다.

<17> 도 17은 도 16에 도시된 Key push modes 파라미터를 표현한 테이블을 도시한 도면이다.

<18> 도 18은 도 16에 도시된 HMAC-Digest 파라미터를 생성할 때 사용되는 입력키를 표현한 테이블을 도시한 도면이다.

<19> 도 19는 도 12에서 가입자 단말이 기지국이 송신한 두 번의 Key Update Command 메시지 중 어느 하나라도 올바르게 수신하지 못하였을 경우의 트래픽 암호화 키 관리 방법에 대한 흐름도이다.

<20> 도 20은 도 19에 도시된 비정상적인 경우의 트래픽 암호화 키 관리 방법에서 가입자 단말의 트래픽 암호화 키 요청 상황에 따른 Key Reply 메시지에 포함되어 전송되는 TEK-Parameters 정보를 나타내는 테이블이다.

<21> 도 21은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에서 트래픽 암호화 키 상태 머신의 상태 천이도이다.

<22> 도 22는 도 21에 도시된 상태 천이를 정리하여 나타낸 테이블이다.

<23> 도 23은 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에서 가입자 단말의 트래픽 암호화 키 상태 머신의 상태 천이도이다.

<24> 도 24는 도 23에 도시된 상태 천이를 정리하여 나타낸 테이블이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<25> 본 발명은 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키(Traffic Encryption Key:TEK) 관리 방법에 관한 것으로, 보다 구체적으로는 무선 휴대 인터넷 시스템에서의 멀티캐스터(Multicast) 서비스와 브로드캐스터(Broadcast) 서비스용 암호화 키 관리 방법 및 그 프로토콜 구성 방법, 그리고 가입자 단말에서의 트래픽 암호화 키 상태 머신의 동작 방법에 관한 것이다.

<26> 무선 휴대 인터넷은 종래의 무선 LAN과 같이 고정된 액세스 포인트(Access Point:AP)를 이용하는 근거리 데이터 통신 방식에 이동성(mobility)을 더 지원하는 차세대 통신 방식이다. 이러한 무선 휴대 인터넷은 다양한 표준들이 제안되고 있으며, 현재 IEEE 802.16을 중심으로 휴대 인터넷의 국제 표준화가 진행되고 있다. 여기서 IEEE 802.16은 기본적으로 도시권 통신망(Metropolitan Area Network, MAN)을 지원하는 규격으로서, 구내 정보 통신망(LAN)과 광역 통신망(WAN)의 중간

정도의 지역을 망라하는 정보 통신망을 의미한다.

<27> 이러한 IEEE 802.16 무선 MAN 시스템에서는 서비스를 안전하게 제공하기 위하여 트래픽 데이터에 대한 암호화 기능을 정의하고 있다. 트래픽 데이터에 대한 암호화 기능은 서비스의 안정성 및 망의 안정성을 위하여 필요한 기본적인 요구사항으로 대두되고 있다.

<28> 현재 IEEE 802.16 무선 MAN 시스템에서는 이와 같은 트래픽 데이터를 암호화하기 위해서 트래픽 암호화 키를 생성하고 분배하는 방식을 정의하였다. 또한, 이 트래픽 암호화 키 또한 보안을 유지하기 위해서 일정 시간이 지나면 갱신하여 새로운 트래픽 암호화 키를 생성 및 분배하도록 하고 있다. 이를 통해, 가입자 단말과 기지국은 동일한 트래픽 암호화 키를 공유한다.

<29> 상기한 인증 및 보안 관련 기능을 수행하기 위해서, 단말과 기지국은 보안 키 관리 프로토콜인 PKM(Privacy Key Management)-REQ(REQuest) 메시지와 PKM-RSP(ReSPonse) 메시지를 사용한다. 단말은 PKM-REQ 메시지 중 한 메시지인 Key Request 메시지를 기지국으로 전송함으로써 새로운 트래픽 암호화 키에 대한 할당을 요구하거나 트래픽 암호화 키 갱신을 요구한다. 한편, 단말로부터 이러한 메시지를 수신한 기지국은 응답으로서 트래픽 암호화 키 할당이나 갱신이 성공하였을 경우에는 PKM-RSP 메시지 중 한 메시지인 Key Reply 메시지를 전송하고, 만약 실패하였을 경우에는 Key Reject 메시지 또는 Auth Invalid 메시지를 해당 단말로 전송한다. 이와 같은 일련의 트래픽 암호화 키 할당 및 갱신 절차를 통해 단말과 기지국 사이에서 공유하게 된 트래픽 암호화 키를 이용하여 무선 구간의 트래픽 데이터

를 암호화 및 복호화하여 송수신하게 된다.

<30> 한편, IEEE 802.16 무선 MAN 시스템에서 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키 갱신 방법은 상기한 바와 같이 유니캐스트(Unicast) 서비스용 트래픽 암호화 키 갱신 방법과 동일하게 처리된다. 즉, 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 갱신 및 분배하는데 있어서, 모든 가입자들이 트래픽 암호화 키 갱신을 요청하고, 이에 대하여 기지국이 동일한 트래픽 암호화 키를 모든 가입자들에게 개별적으로 응답을 함으로써 트래픽 암호화 키 갱신 및 분배가 이루어지므로 무선 구간 신호 채널의 사용 부하가 매우 커지게 된다. 따라서, 유니캐스트 서비스용 트래픽 암호화 키 갱신 방법과 동일한 절차로 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 갱신하는 것은 무선 채널 자원을 불필요하게 사용하게 되는 문제점이 발생한다. 이에 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키 갱신에 따른 무선 채널 자원을 효과적으로 감소시키는 절차가 요구된다.

【발명이 이루고자 하는 기술적 과제】

<31> 따라서, 본 발명의 목적은 상기한 문제점을 해결하고자 하는 것으로, 무선 휴대 인터넷 시스템에서 멀티캐스트 서비스와 브로드캐스트 서비스용 트래픽 암호화 키를 갱신할 때 기지국에서 자동으로 트래픽 암호화 키를 갱신하여 방송 채널을 사용하여 전달함으로써 멀티캐스트 서비스와 브로드캐스트 서비스용 트래픽 암호화 키를 갱신하는데 있어서 무선 구간 신호 채널의 사용 부하를 감소시키는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법 및 그 프로토콜 구성 방법, 그리

고 가입자 단말에서의 트래픽 암호화 키 상태 머신의 동작 방법을 제공하는 것이다.

【발명의 구성】

<32> 상기 과제를 달성하기 위한 본 발명의 하나의 특징에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법은,

<33> 무선 휴대 인터넷 시스템에서 기지국이 무선 연결된 가입자 단말에 대한 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하는 방법으로서,

<34> a) 상기 가입자 단말과 현재 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 특정 시간이 경과한 때, 상기 현재의 트래픽 암호화 키를 갱신하기 위해 새로운 트래픽 암호화 키를 생성하는 단계; 및 b) 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 브로드캐스트 커넥션(Broadcast Connection)을 통해 상기 생성된 새로운 트래픽 암호화 키를 송신하여 상기 가입자 단말에서 사용되는 트래픽 암호화 키가 갱신되도록 하는 단계를 포함한다.

<35> 본 발명의 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법은,

<36> 무선 휴대 인터넷 시스템에서 기지국이 무선 연결된 가입자 단말에 대한 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 송수신하는 트

래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하는 방법으로서,

<37> a) 상기 가입자 단말과 현재 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 특정 시간이 경과하기 전에 트래픽 암호화 키를 암호화하거나 복호하는데 사용되는 특정 키를 생성하는 단계; b) 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 프라이머리 매니지먼트 커넥션(Primary Management Connection)을 통해 상기 생성된 특정 키를 각각 송신하는 단계; c) 상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 상기 특정 시간이 경과한 때, 상기 현재의 트래픽 암호화 키를 갱신하기 위해 새로운 트래픽 암호화 키를 생성하는 단계; 및 d) 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 브로드캐스트 커넥션(Broadcast Connection)을 통해 상기 생성된 새로운 트래픽 암호화 키를 송신-여기서 송신되는 트래픽 암호화 키는 상기 b) 단계에서 송신된 새로운 특정 키로 암호화되어 있음-하여 상기 가입자 단말에서 사용되는 트래픽 암호화 키가 갱신되도록 하는 단계를 포함한다.

<38> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법은,

<39> 무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용하는 트래픽 암호화 키를 관리

하는 방법으로서,

<40> a) 상기 기지국으로부터 브로드캐스트 커넥션(Broadcast Connection)을 통해 새로운 트래픽 암호화 키를 수신하는 단계; 및 b) 상기 수신된 새로운 트래픽 암호화 키로 현재의 트래픽 암호화 키를 갱신하여 이후부터 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 상기 갱신된 새로운 트래픽 암호화 키를 사용하는 단계를 포함한다.

<41> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법은,

<42> 무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용하는 트래픽 암호화 키를 관리하는 방법으로서,

<43> a) 상기 기지국으로부터 트래픽 암호화 키를 복호하는데 사용되는 새로운 특정 키를 프라이머리 매니지먼트 커넥션(Primary Management Connection)을 통해 수신하는 단계; b) 상기 수신된 새로운 특정 키로 현재의 특정 키를 갱신하는 단계; c) 상기 기지국으로부터 브로드캐스트 커넥션(Broadcast Connection)을 통해 새로운 트래픽 암호화 키－여기서 새로운 트래픽 암호화 키는 상기 b) 단계에서 수신된 새로운 특정 키로 암호화되어 있음－를 수신하는 단계; 및 d) 상기 수신된 새로운 트래픽 암호화 키를 상기 b) 단계에서 수신된 새로운 특정 키로 복호하여 현재의 트래픽 암호화 키를 갱신하고, 이후부터 상기 기지국과 송수신하는 트래픽 데이터

를 암호화 또는 복호하는데 상기 갱신된 새로운 트래픽 암호화 키를 사용하는 단계를 포함한다.

<44> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법은,

<45> 무선 휴대 인터넷 시스템에서 가입자 단말과 기지국 간에 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키에 대한 관리를 수행하기 위한 프로토콜을 구성하는 방법으로서,

<46> a) 상기 가입자 단말이 트래픽 암호화 키를 최초로 요청하기 위해 MAC 메시지인 키 요청 메시지(Key Request)를 이용하여 상기 기지국으로 송신하는 단계; b) 상기 기지국이 수신한 키 요청 메시지의 응답으로 트래픽 암호화 키를 전달하기 위해 키 응답(Key Reply) 메시지를 송신하는 단계; 및 c) 상기 기지국이 트래픽 암호화 키를 자동적으로 갱신하고 이를 키 응답(Key Reply) 메시지를 이용하여 모든 단말에게 방송 채널을 통해 전송하는 단계를 포함한다.

<47> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법은,

<48> 무선 휴대 인터넷 시스템에서 가입자 단말과 기지국 간에 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키에 대한 관리를 수행하기 위한 프로토콜을 구성하는 방법으로서,

<49> a) 상기 가입자 단말이 트래픽 암호화 키를 최초로 요청하기 위해 MAC 메시지인 키 요청(Key Request) 메시지를 이용하여 상기 기지국으로 송신하는 단계; b) 상기 기지국이 수신한 키 요청 메시지의 응답으로 트래픽 암호화 키와 특정 키-여기서 특정 키는 상기 트래픽 암호화 키를 암호화하는데 사용됨-를 전달하기 위해 MAC 메시지인 키 응답(Key Reply) 메시지를 상기 가입자 단말로 송신하는 단계; c) 상기 특정 키를 갱신하기 위해 상기 기지국이 새로운 특정 키를 포함하는 제1 키 갱신 명령(Key Update Command) 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계; 및 d) 상기 트래픽 암호화 키를 갱신하기 위해 상기 기지국이 새로운 트래픽 암호화 키-여기서 새로운 트래픽 암호화 키는 상기 새로운 특정 키에 의해 암호화됨-를 포함하는 제2 키 갱신 명령 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계를 포함한다.

<50> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서 단말의 트래픽 암호화 키 상태 머신 동작 방법은,

<51> 무선 휴대 인터넷 시스템에서 가입자 단말에 구비되며, 상기 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하기 위한 단말의 트래픽 암호화 키 상태 머신의 동작 방법으로서,

<52> 상기 단말이 기지국으로 트래픽 암호화 키를 최초로 요청하는 키 요청 메시지 송신 이벤트(event)에 의해 키 요청(Key Request) 메시지를 송신하고 대기하는

동작 대기 단계(Op Wait); 상기 기지국과의 정상적인 트래픽 데이터의 송수신 동작을 수행하는 동작 단계(Operational)를 포함하며, 상기 단말의 트래픽 암호화 키 상태 머신에서, 상기 동작 단계에서 상기 기지국에서 트래픽 암호화 키를 자동적으로 생성하고 이를 상기 단말들로 방송 채널을 통해 키 응답(Key Reply) 메시지를 송신하고 단말이 이를 수신하여 다시 동작 단계에 머무르는 것을 특징으로 한다.

<53> 본 발명의 또 다른 특징에 따른 무선 휴대 인터넷 시스템에서단말의 트래픽 암호화 키 상태 머신 동작 방법은,

<54> 무선 휴대 인터넷 시스템에서 가입자 단말에 구비되며, 상기 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하기 위한 단말의 트래픽 암호화 키 상태 머신의 동작 방법으로서,

<55> 상기 단말이 기지국으로 트래픽 암호화 키를 최초로 요청하는 키 요청 메시지 송신 이벤트(event)에 의해 키 요청(Key Request) 메시지를 송신하고 대기하는 동작 대기 단계(Op Wait); 상기 기지국과의 정상적인 트래픽 데이터의 송수신 동작을 수행하는 동작 단계(Operational); 및 상기 기지국에서 자동으로 생성되어 송신되는 새로운 트래픽 암호화 키를 갱신하기 위해 대기하는 M&B(Multicast & Broadcast) 갱신 잠정 대기 단계(M&B Rekey Interim Wait)를 포함하며, 상기 트래픽 암호화 키 상태 머신은, 상기 동작 단계에 있는 상기 단말이 상기 기지국으로부터 트래픽 암호화 키를 암호화 및 복호화하는데 사용되는 특정 키가 포함된 제1 키

갱신 명령 메시지를 수신하였다는 이벤트 발생에 의해 상기 M&B 갱신 잠정 대기 단계로 천이하여 동작하고, 이 M&B 갱신 잠정 대기 단계에서 상기 기지국으로부터 트래픽 암호화 키가 포함된 제2 키 갱신 명령 메시지를 수신하였다는 이벤트 발생에 의해 상기 동작 단계로 재천이하여 동작하는 것을 특징으로 한다.

<56> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였다. 명세서 전체를 통하여 유사한 부분에 대해서는 동일한 도면 부호를 붙였다.

<57> 이하, 첨부된 도면을 참조하여 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에 대해서 상세하게 설명한다.

<58> 도 1은 본 발명이 적용되는 무선 휴대 인터넷의 개요를 도시한 개략도이다.

<59> 도 1에 도시된 바와 같이, 무선 휴대 인터넷 시스템은 기본적으로 가입자 단말(Subscribe Station, 10), 가입자 단말(10)과 무선 통신을 수행하는 기지국(Base Station, 20, 21), 기지국(20, 21)에 접속되어 게이트웨이를 통해 접속된 라우터(30, 31) 및 라우터(30, 31)에 접속되어 가입자 단말(20, 21)에 대한 인증을 수행하는 인증 서버(AAA:Authentication Authorization and Accounting) 서버(40)를 포함한다.

<60> 종래의 IEEE 802.11과 같은 무선 LAN 방식은 고정된 액세스 포인트를 중심으

로 근거리내에서 무선 통신이 가능한 데이터 통신 방식을 제공하고 있으나, 이는 가입자 단말의 이동성을 제공하는 것이 아니고, 단지 유선이 아닌 무선으로 근거리 데이터 통신을 지원한다는 한계를 가지고 있었다.

<61> 한편, IEEE 802.16 그룹 등에서 추진중인 무선 휴대 인터넷 시스템은 도 1에 도시된 가입자 단말(10)이 기지국(20)이 관장하는 셀에서 기지국(21)이 관장하는 셀로 이동하는 경우에도 그 이동성을 보장하여 끊기지 않는 데이터 통신 서비스를 제공하게 된다.

<62> 따라서, 무선 휴대 인터넷 시스템은 이동통신 서비스와 같이 가입자 단말(10)의 핸드오버를 지원하며, 가입자 단말의 이동에 따라 동적인 IP 어드레스 할당도 가능하다.

<63> 여기서, 무선 휴대 인터넷 가입자 단말(10)과 기지국(20, 21)은 직교 주파수 분할 다중화(Orthogonal Frequency Division Multiple Access; 이하 OFDMA라고 함)방식으로 통신을 수행한다. OFDMA 방식은 복수의 직교주파수의 부반송파(sub carrier)를 복수의 서브 채널로 이용하는 주파수 분할 방식과, 시분할 방식(TDM) 방식을 결합한 다중화 방식이다. 이러한 OFDMA 방식은 본질적으로 다중 경로(multi path)에서 발생하는 페이딩(fading)에 강하며, 데이터 전송률이 높다.

<64> 도 2는 도 1에 도시된 무선 휴대 인터넷 시스템의 계층 구조를 도시한 계층도이다.

<65> 도 2에 도시된 바와 같이, IEEE 802.16의 무선 휴대 인터넷 시스템의 계층 구조는 크게 물리 계층(Physical Layer, L10)과 매체 접근 제어(Media Access

Control; 이하 "MAC" 이라고 함) 계층(L21, L22, L23)으로 구분된다.

<66> 물리 계층(L10)은 변복조 및 코딩 등 통상의 물리 계층에서 수행하는 무선 통신 기능을 담당하고 있다.

<67> 한편, 무선 휴대 인터넷 시스템은 유선 인터넷 시스템과 같이 그 기능별로 세분화된 계층을 가지지 않고 하나의 MAC 계층에서 다양한 기능을 담당하게 된다.

<68> 그 기능별로 서브 계층을 살펴보면, MAC 계층은 프라이버시 서브계층 (Privacy Sublayer, L21), MAC 공통부 서브계층(MAC Common Part Sublayer, L22), 서비스 특정 집합 서브계층(Service Specific Convergence Sublayer, L23)을 포함한다.

<69> 프라이버시 서브계층(L21)은 장치 인증 및 보안키 교환, 암호화 기능을 수행한다. 프라이버시 서브계층(L21)에서 장치에 대한 인증만이 수행되고, 사용자 인증은 MAC의 상위 계층(도시 생략)에서 수행된다.

<70> MAC 공통부 서브계층(L22)은 MAC 계층의 핵심적인 부분으로서 시스템 액세스, 대역폭 할당, 트래픽 연결(Traffic Connection) 설정 및 유지, QoS 관리에 관한 기능을 담당한다.

<71> 서비스 특정 집합 서브계층(L23)은 연속적인 데이터 통신에 있어서, 페이로드 헤더 서프레션(suppression) 및 QoS 맵핑 기능을 담당한다.

<72> 도 3은 도 1에 도시된 무선 휴대 인터넷 시스템에서 기지국(20, 21)과 가입자 단말(10)의 연결구조를 도시한 개략도이다.

<73> 도 3에 도시된 바와 같이, 가입자 단말(10)의 MAC 계층과 기지국(20, 21)의 MAC 계층은 연결(Connection, C1)이라는 개념이 존재한다.

<74> 여기서, "연결(C1)"이란 용어는 물리적 연결관계가 아니라 논리적 연결관계를 의미하는 것으로서, 신호 메시지들을 송수신하기 위해 또는 하나의 서비스 플로우에 대하여 트래픽을 전송하기 위해 가입자 단말(10)과 기지국(20, 21)의 MAC 동위계층(peer)들 사이의 맵핑 관계로 정의된다.

<75> 따라서, 임의의 메시지와 메시지에 포함된 파라미터를 통해 설정된 각종 상기 연결들이 관리되고, 상기 연결을 통하여 전달되어지는 신호 메시지나 트래픽 데이터에 따라 각각의 기능을 수행하게 되는 것이다.

<76> 그 밖에도 MAC 메시지는 각종 동작에 대한 요청(REQ), 응답(RSP), 확인(ACK)기능을 수행하는 다양한 메시지를 포함한다.

<77> 도 4는 도 1에 도시된 무선 휴대 인터넷 시스템에서의 가입자 단말과 기지국 간의 연결 설정을 위한 흐름도이다.

<78> 도 4를 참조하면, 가입자 단말(10)이 기지국(20)에 진입하면(S10), 우선 가입자 단말(10)은 기지국(20)과 하향링크 동기를 설정하고, 상향링크 파라미터를 획득하게 된다(S20). 예를 들어, 상기 파라미터는 물리 계층의 특성(예를 들어, 신호대 잡음비)에 따른 채널 디스크립터 메시지를 포함할 수 있다.

<79> 그 후, 가입자 단말(10)과 기지국(20)은 레인징(Ranging) 절차를 수행한다(S30). 여기서 레인징은 가입자 단말(10)과 기지국(20) 간의 타이밍, 전력, 주파수 정보를 정정하여 일치시키는 것으로서, 최초에 초기 레인징(initial ranging)을

수행하고, 이후 CDMA 코드를 이용한 주기적으로 주기적 레인징(periodic ranging)을 수행하게 된다.

<80> 이러한 레인징 절차(S30)가 완료되면, 가입자 단말(10)과 기지국(20) 간의 연결 설정을 위한 단말 기본 기능에 관한 협상이 수행된다(S40). 이러한 기본 기능에 대한 협상이 완료되면, 기지국의 가입자 단말의 인증서(Certificate)를 이용하여 가입자 단말 인증이 수행된다(S50).

<81> 가입자 단말(10)의 인증이 완료되어 무선 휴대 인터넷의 사용 권한이 확인되면, 단말과 기지국은 설정된 각각의 연결(C1)마다 트래픽 암호화 키를 공유하기 위해서 트래픽 암호화 키 생성 및 분배하는 절차를 수행한다(S60). 가입자 단말(10)에 대한 인증 및 트래픽 암호화 키 분배 절차가 완료된 후 기지국(20)은 가입자 단말(10)의 MAC 계층 관련된 기능들을 협상 및 등록한다(S70). 그 후, 기지국(20)은 DHCP 서버 또는 MIP 서버를 통해 IP 주소를 가입자 단말(20)에 제공하여 IP 연결 설정을 수행한다(S80).

<82> IP 주소를 부여받은 가입자 단말에게 본격적인 트래픽 서비스를 제공하기 위해서 단말(10)과 기지국(20)은 서비스 플로우 각각에 대한 트래픽 연결 설정을 수행한다(S90).

<83> 이와 같이, 상기 단계들을 통해, 무선 휴대 인터넷 시스템에서는 가입자 단말(10, 20)이 임의의 멀티캐스트 서비스나 브로드캐스트 서비스를 실질적으로 제공받기 위해서 우선 해당 트래픽 데이터를 암호화하는데 필요한 트래픽 암호화 키를 분배받아야 한다. 여기에서 모든 멀티캐스트 서비스나 브로드캐스트 서비스에는

각각의 서비스 트래픽 데이터를 암호화하기 위해 개별적인 트래픽 암호화 키가 존재한다. 다시 말해서, 모든 멀티캐스트 서비스용 트래픽 암호화 키가 서로 다르고, 브로드캐스트 서비스용 트래픽 암호화 키와도 달라야 한다. 이는 하나의 멀티캐스트 서비스에 대한 트래픽 암호화 키를 가입자 단말이 안다고 할지라고 다른 멀티캐스트 서비스를 제공받을 수 없도록 하기 위함이고, 단말들이 다른 서비스 사업자를 통해 제공되는 브로드캐스트 서비스를 제공받는 것을 방지하기 위함이다.

<84> 도 5는 일반적인 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법의 흐름도이다.

<85> 도 5를 참조하면, 먼저 가입자 단말(10)은 멀티캐스트 서비스 또는 브로드캐스트 서비스에 대한 트래픽 암호화 키를 최초로 할당받기 위해 기지국(20)으로 PKM-REQ 메시지인 키 요청(Key Request) 메시지를 송신한다(S100).

<86> 여기서, 트래픽 암호화 키, 트래픽 암호화 키 일련번호, 트래픽 암호화 키 유효 시간, 암호화 알고리즘 등을 나타내는 파라미터를 포함하는 집합을 하나의 SA(Security Association)로 표현하고, 이 SA에는 식별자 기능을 하는 SA-ID(Security Association-IDentification)도 포함되어 있다. 멀티캐스트 서비스나 브로드캐스트 서비스는 서로 다른 하나의 SA와 관련되어 있다. 다시 말해서, 임의의 동일한 멀티캐스트 서비스를 제공받는 단말들은 동일한 하나의 SA 정보를 가지고 있고, 브로드캐스트 서비스를 제공받는 단말들도 동일한 하나의 SA 정보를 가지고 있지만, 이들 멀티캐스트 서비스나 브로드캐스트 서비스와 관련된 SA가 서로 독립적이기 때문에 이들 개별 서비스 하나당 하나의 SA와 관련있다고 간주할 수

있다. 따라서, 키 요청 메시지에는 해당 서비스와 관련된 SA의 식별자인 SA-ID가 포함되어 있으며, 도 5에 도시된 바와 같이 n 번째 SA-ID에 해당하는 트래픽 암호화 키와 그에 따른 정보들을 기지국(20)에게 요청하는 것이다.

<87> 또한, 가입자 단말(10)이 기지국(20)으로 전송하는 키 요청 메시지의 MAC 헤더에는 프라이머리 매니지먼트 커넥션(Primary Management Connection)을 위한 Primary Management CID가 사용된다. 이 Primary Management CID는 기지국(20)이 가입자 단말(10)의 초기 접속시 단말마다 고유하게 할당해주는 CID로써 단말을 구별해줄 수 있다.

<88> 가입자 단말(10)로부터 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키 생성 및 분배를 요청하는 Key Request 메시지를 수신한 기지국(20)은 수신된 메시지의 모든 필드 값들을 바탕으로 하여 트래픽 암호화 키 생성 메커니즘으로 해당 가입자 단말(10)에 할당할 x 번째 트래픽 암호화 키(TEK_x)를 생성한 후 가입자 단말(10)로 키 응답 메시지인 Key Reply 메시지를 통해 전송한다(S110). 이때, 가입자 단말(10)이 n 번째 SA를 요구하였기 때문에 기지국(20)은 n 번째 SA들을 키 응답 메시지에 포함시켜 전송하는 것이다. 이 때의 키 응답 메시지의 MAC 헤더에는 트래픽 암호화 키를 요청하였던 가입자 단말(10)에게만 전송해야 하므로 Key Request 메시지의 MAC 헤더에 포함되었던 Primary Management CID를 그대로 사용한다. 이로써 가입자 단말(10)이 임의의 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 최초로 분배받는 절차가 완료되는 것이다.

<89> 이와 같이 기지국에 의해 생성된 n 번째 SA에 대한 x 번째 트래픽 암호화 키를 가지고 가입자 단말(10)은 해당 서비스의 트래픽 데이터를 복호화하는 것이다. 또한, 가입자 단말(10)이 트래픽 암호화 키를 Key Reply 메시지를 통해 기지국(20)으로부터 분배받자마자 해당 트래픽 암호화 키의 실제 유효 시간(TEK Active Lifetime)이 도 5에 도시된 바와 같이 시작된다(S120).

<90> 그 후 가입자 단말(10)은 끊임없이 안전하게 트래픽 서비스를 제공받기 위해서 주기적으로 트래픽 암호화 키를 갱신해야 한다. 이를 위해 가입자 단말(10)은 내부적으로 TEK Grace Time을 관리한다. 이 TEK Grace Time은 이전에 할당 받았던 트래픽 암호화 키가 만료되기 전에 가입자 단말(10)이 트래픽 암호화 키 갱신 요청을 유발하는 시점을 의미한다. 즉, 가입자 단말(10)은 이 TEK Grace Time이 작동하게 되면(S130) TEK Refresh Timeout 이벤트를 발생시킨다(S140). 가입자 단말(10) 내부에는 이러한 TEK Refresh Timeout 이벤트를 수행할 트래픽 암호화 키 상태 머신이 소프트웨어로 구현되어 있다.

<91> 이러한 TEK Refresh Timeout 이벤트(S140)로 인해 가입자 단말(10)은 기지국(20)으로 트래픽 암호화 키 갱신 및 분배를 위한 키 요청 메시지인 Key Request 메시지를 전송한다(S150). 이 때, 전송되는 Key Request 메시지는 상기 단계(S100)에서 최초로 트래픽 암호화 키를 요청하였던 Key Request 메시지와 동일한 SA-ID, Primary Management CID 등이 포함된다.

<92> 마찬가지로, 트래픽 암호화 키 갱신 및 분배를 요청하는 Key Reuqest 메시지

를 수신한 기지국(20)은 응답 메시지로써 x+1 번째 트래픽 암호화 키(TEK_{x+1})를 생성하고 이 트래픽 암호화 키를 Key Reply 메시지에 포함시켜 해당 가입자 단말(10)로 전송한다(S160). 이 때, Key Reply 메시지의 MAC 헤더에도 상기 단계(S110)에서 트래픽 암호화 키를 최초로 분배하였던 Key Reply 메시지의 MAC 헤더에서 사용하였던 Primary Management CID가 포함되고, Key Request 메시지(S150)에서의 SA-ID값이 n이기 때문에 Key Reply 메시지에는 마찬가지로 n 번째의 SA가 포함된다. 그러나 상기 단계(S110)에서와 달리 이 SA에는 기지국이 x+1 번째로 생성한 트래픽 암호화 키(TEK_{x+1})가 존재한다.

<93> 그 후, 가입자 단말(10)이 기지국(20)으로부터 x+1 번째로 생성된 트래픽 암호화 키를 Key Reply 메시지로 분배 받자마자 해당 x+1 번째의 트래픽 암호화 키의 실제 유효 시간이 시작된다(S170). 이후부터 제공받은 해당 서비스 데이터는 x+1 번째의 트래픽 암호화 키를 가지고 복호화된다. 이로써, 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 갱신 및 분배하는 절차가 완료되고, 계속 반복되는 것이다.

<94> 상기한 바와 같이, IEEE 802.16 무선 MAN 시스템과 같은 무선 휴대 인터넷 시스템에서 지원하는 트래픽 암호화 키를 갱신하기 위해서는 가입자 단말(10)이 기지국(20)으로 전송하는 26바이트의 Key Request 메시지와 기지국(20)이 가입자 단말(10)로 전송하는 최대 84바이트의 Key Reply 메시지가 사용되어, 결과적으로, 트래픽 암호화 키의 유지를 위한 키 갱신 및 분배를 위해서 가입자 단말(10)과 기지

국(20) 간에 총 110바이트의 신호 메시지가 사용된다.

<95> 도 6은 일반적인 무선 휴대 인터넷 시스템에서 복수의 가입자 단말과 기지국 간의 트래픽 암호화 키 갱신 방법의 흐름도이다.

<96> 도 6에 도시된 단말(10-1, 10-2, 10-3, …, 10-z)들은 기지국(20)으로부터 하나의 동일한 멀티캐스트 서비스 또는 동일한 브로드캐스트 서비스를 현재 제공받고 있는 단말들이다. 여기서, 하나의 멀티캐스트 서비스나 브로드캐스트 서비스가 n 번째 SA와 관련되어 있다고 가정한다.

<97> 이미 최초 키 생성 과정 또는 이전의 키 갱신 과정을 거쳐 암호화 키를 분배받은 모든 단말들(10-1, 10-2, 10-3, …, 10-z)에서 각각 내부적으로 저장하고 있는 동일한 TEK Grace Time에 의해 TEK Refresh Timeout 이벤트가 발생하고, 이러한 TEK Refresh Timeout에 의해 각각 n 번째 SA의 트래픽 암호화 키를 갱신받기 위해서 모든 단말들(10-1, 10-2, 10-3, …, 10-z)이 Key Request 메시지를 각각 기지국(20)으로 전송한다(S150-1, S150-2, S150-3, …, S150-z).

<98> 이 때, 모든 단말(10-1, 10-2, 10-3, …, 10-z)들의 n 번째 SA에 해당하는 TEK Grace Time 시점이 동일하기 때문에 모든 단말(10-1, 10-2, 10-3, …, 10-z)로부터의 Key Request 메시지들이 거의 한 순간에 기지국(20)으로 전송된다. 이 때 모든 단말(10-1, 10-2, 10-3, …, 10-z)이 전송하는 Key Request 메시지에는 값이 n인 SA-ID가 포함된다. 하지만, 이 Key Request 메시지의 MAC 헤더에는 단말이 초기 접속 시 기지국으로부터 단말마다 고유하게 할당받은 서로 다른 Primary Management CID가 사용된다.

<99> 이와 같이, z개의 단말(10-1, 10-2, 10-3, …, 10-z)이 현재 서비스를 받고 있는 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키 갱신 요청 메시지를 전송하기 위해서 동일한 시간에 무선 채널 구간에 하나의 서비스당 26×z 바이트가 사용된다.

<100> 다음, z개의 단말(10-1, 10-2, 10-3, …, 10-z)로부터 n 번째 SA의 트래픽 암호화 키 갱신 요청 메시지를 각각 수신받은 기지국(20)은 n 번째 SA의 트래픽 암호화 키를 갱신하고, 응답 메시지로써 n 번째 SA가 포함된 Key Reply 메시지를 모든 단말(10-1, 10-2, 10-3, …, 10-z)에게 동시에 각각 전송한다(S160-1, S160-2, S160-3, …, S160-z). 이 때 전송하는 Key Reply 메시지의 MAC 헤더에는 각각의 단말(10-1, 10-2, 10-3, …, 10-z)에게 할당된 Primary Management CID가 사용된다. 기지국(20)은 특정 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 분배하기 위해서는 모든 단말(10-1, 10-2, 10-3, …, 10-z)에게 일일이 Key Reply 메시지를 전송해야 하기 때문에 무선 채널 구간에서 84×z 바이트가 사용된다.

<101> 다시 말해서, 특정 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받는 모든 단말(10-1, 10-2, 10-3, …, 10-z)은 동일한 하나의 트래픽 암호화 키를 기지국(20)으로부터 각각 분배받아 해당 서비스 트래픽 데이터를 복호화할 때 사용한다. 그러나, 동일한 트래픽 암호화 키를 갱신하는데 있어서 모든 단말(10-1, 10-2, 10-3, …, 10-z)이 각각 갱신 요청을 하고, 이에 대한 응답으로 기지국(20)이 모든 단말(10-1, 10-2, 10-3, …, 10-z)에게 일일이 갱신된 트래픽 암호화 키를 분배하는

방식은 비효율적이다. 예를 들어, 하나의 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받고 있는 단말이 상기와 같이 z개라면 해당 서비스용 트래픽 암호화 키를 갱신하는데 총 110×z 바이트가 필요하다. 이는 무선 채널의 신호 자원의 과다한 낭비로 귀결된다.

<102> 즉, 이처럼 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 갱신하는데 있어서, 유니캐스트 서비스용 트래픽 암호화 키를 갱신하는 방법과 같이 모든 단말(10-1, 10-2, 10-3, …, 10-z)이 해당 서비스의 트래픽 암호화 키 갱신을 유발하여 요청하고, 이 요청에 대하여 기지국(20)이 모든 단말(10-1, 10-2, 10-3, …, 10-z)에게 각각 분배하는 것은 임의의 짧은 순간에 무선 채널의 신호 자원을 많이 낭비하는 것이고, 또한 기지국(20)의 불필요한 처리량을 야기하는 것이 된다.

<103> 따라서, 본 발명의 실시예에서는 상기한 문제점을 해결하기 위해, 기지국이 가입자 단말에게 생성하여 분배한 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키가 만료되기 전에 기지국이 해당 서비스의 트래픽 암호화 키를 자동으로 갱신하여 해당되는 가입자 단말에게 방송 신호 채널을 통해 먼저 전송하여 분배하는 것을 특징으로 한다.

<104> 이를 위해 기지국은 도 7에 도시된 바와 같이 본 발명의 실시예에 따라 특정된 시간을 정의하여 사용한다.

<105> 도 7은 본 발명의 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 갱신을 위한 암호 관련 PKM 파라미터 운용 범위를 나타낸 테이블을 도시한

도면이다.

<106> 이러한 PKM 파라미터 테이블에는 M&B(Multicast & Broadcast) TEK Grace Time이 추가되며, 이러한 M&B TEK Grace Time은 기지국이 내부적으로 저장하고 있는 파라미터로써, 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키가 만료되기 전에 기지국이 해당 서비스의 트래픽 암호화 키를 갱신을 시작하는 시점을 의미한다. 이 M&B TEK Grace Time은 단말이 트래픽 암호화 키가 만료되기 전에 갱신을 시작하는 시점을 의미하는 TEK Grace Time보다 큰 값을 가져야 한다. 그 이유로는, 단말에서 TEK Grace Time의 작동에 의해 기지국으로 키 갱신을 위한 메시지가 전송되기 전에 기지국에서 해당 서비스에 대한 트래픽 암호화 키를 갱신하여 단말로 전송해야 하기 때문이다.

<107> 도 8은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법의 흐름도이다.

<108> 도 8을 참조하면, 먼저 가입자 단말이 임의의 멀티캐스트 서비스나 브로드캐스트 서비스를 실질적으로 받기 전에 우선 해당 서비스 트래픽 데이터를 복호하는데 필요한 트래픽 암호화 키를 분배받아야 한다. 이와 같이 가입자 단말이 기지국으로부터 최초로 해당 서비스의 트래픽 암호화 키를 분배받는 과정(S200, S210)은 도 5를 참조하여 설명한 가입자 단말의 최초 트래픽 암호화 키 요청 및 분배 과정(S100, S110)과 동일하므로 여기에서는 상세한 설명을 생략한다.

<109> 이와 같이, 가입자 단말기가 기지국으로부터 n 번째 SA에 대해 x 번째로 생성한 해당 서비스의 트래픽 암호화 키가 포함된 Key Reply 메시지를 수신받은 때부

터 x 번째의 트래픽 암호화 키의 실제 유효 시간이 시작되고(S220), 이 유효 시간 동안 가입자 단말은 해당 서비스를 제공받을 때 x 번째 트래픽 암호화 키를 가지고 트래픽 데이터를 복호하여 사용한다.

<110> 한편, 해당 서비스의 트래픽 데이터를 끊임없이 안전하게 기지국이 가입자 단말에게 제공하기 위해서 n 번째 SA의 트래픽 암호화 키를 주기적으로 갱신해야 한다.

<111> 그러나, 본 발명의 제1 실시예에서는 도 5를 참조하여 설명한 바와 같이 일반적인 무선 휴대 인터넷 시스템에서처럼 가입자 단말이 TEK Grace time에 의한 트래픽 암호화 키 갱신을 유발하지 않고, 기지국이 해당 서비스 트래픽 암호화 키를 주기적으로 갱신하는 것이다. 이를 위해 기지국은 내부적으로 도 7을 참조하여 설명한 바와 같은 M&B TEK Grace Time 파라미터를 관리하고 있는데, 멀티캐스트 서비스나 브로드캐스트 서비스별로 이 M&B TEK Grace Time 시점이 시작되면(S230), 기지국은 M&B TEK Refresh Timeout 이벤트를 발생시킨다(S240). 기지국 내부에는 이러한 M&B TEK Refresh Timeout 이벤트를 수행할 트래픽 암호화 키 상태 머신이 소프트웨어로 구현되어 있다. 따라서, 기지국은 이러한 M&B TEK Refresh Timeout 이벤트로 인해 트래픽 암호화 키 상태 머신을 통해 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 새롭게 갱신하게 된다. 이 때 갱신되는 트래픽 암호화 키는 x+1 번째 트래픽 암호화 키가 된다.

<112> 그 후, 기지국은 단말에게 n 번째 SA에 대해 갱신된 x+1 번째 트래픽 암호화 키를 포함하는 Key Reply 메시지를 전송한다(S250).

<113> 이와 같이, 기지국으로부터 트래픽 암호화 키를 포함한 Key Reply 메시지를 수신한 가입자 단말은 내부적으로 관리하고 있는 TEK Grace Time이 동작하지 않게 된다. 즉, 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받는 가입자 단말은 유니캐스트 서비스와 달리 해당 서비스에 대한 특별한 트래픽 암호화 키 요청없이 트래픽 암호화 키를 분배받게 되는 것이다.

<114> 이 후, 가입자 단말이 x+1 번째로 생성된 트래픽 암호화 키를 Key Reply 메시지를 통해 기지국으로부터 분배 받자마자 해당 x+1 번째의 트래픽 암호화 키 실제 유효 시간이 시작된다(S260). 이후부터 가입자 단말과 기지국은 제공받은 해당 서비스 데이터에 대해 x+1 번째의 트래픽 암호화 키를 가지고 암호화 및 복호화하는 것이다.

<115> 한편, 기지국이 가입자 단말로 전송하는 Key Reply 메시지의 MAC 헤더에는 브로드캐스트 CID가 사용됨으로써, 한 번의 Key Reply 메시지로 해당 서비스를 수행하는 모든 단말에게 갱신된 트래픽 암호화 키를 브로드캐스트 커넥션(Broadcast Connection)을 통해 효율적으로 분배할 수 있다. 특히, 브로드캐스트 커넥션을 통해 전송하는 Key Reply 메시지에 포함된 트래픽 암호화 키가 어떠한 멀티캐스트 서비스 데이터를 암호화하는데 필요한 트래픽 암호화 키인지 또는 어떠한 브로드캐스트 서비스 데이터를 암호화하는데 필요한 트래픽 암호화 키인지를 구별해야 하는데, 이는 Key Reply 메시지에 포함된 SA의 식별자인 SA-ID로 구별된다. 예를 들어, 도 8에서 기지국으로부터 갱신되어 분배되는 Key Reply 메시지에 포함된 x+1 번째 트래픽 암호화 키는 n 번째 SA로써 이 SA와 관련된 서비스를 암호화하는데 사

용됨을 알 수 있고, 이 SA와 관련된 서비스를 사용하는 가입자 단말들만이 이 x+1 번째 트래픽 암호화 키를 수신하여 사용한다.

<116> 여기서, 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 기지국이 자체적으로 갱신하는 방식에서 사용되는 Key Reply 메시지는 최대 55바이트이다.

<117> 도 9는 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서 가입자 단말이 기지국이 갱신하여 브로드캐스트 커넥션을 통해 전송한 갱신된 트래픽 암호화 키가 포함된 Key Reply 메시지를 올바르게 수신하지 못하였을 경우에 있어서 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법의 흐름도이다.

<118> 가입자 단말이 멀티캐스트 서비스나 브로드캐스트 서비스에 대한 트래픽 암호화 키를 최초로 요청하여 분배받는 과정(S200, S210)부터, 기지국에서 M&B TEK Grace Time이 시작되어 기지국에서 자동으로 트래픽 암호화 키를 갱신하여 가입자 단말로 브로드캐스트 커넥션을 통해 전송하는 과정(S220 ~ S250)을 통해 가입자 단말이 기지국에 의해 갱신된 트래픽 암호화 키를 분배받게 되지만, 가입자 단말이 이러한 메시지를 기지국으로부터 정상적으로 수신하지 못하였을 경우, 즉 비정상적으로 트래픽 암호화 키를 분배받지 못한 단말들은 도 1을 참조하여 설명한 바와 같이 가입자 단말들 개별적으로 트래픽 암호화 키를 갱신 요청하여 기지국으로부터 분배받는 과정을 거친다. 즉, 비정상적으로 트래픽 암호화 키를 분배받지 못한 가입자 단말들은 내부적으로 관리하고 있는 TEK Grace Time이 동작하게 되고(S270), 이 TEK Grace Time이 동작하는 단말들은 내부 트래픽 암호화 키 상태 머신에 TEK

Refresh Timeout 이벤트가 발생한다(S280). 이러한 이벤트로 인해 비정상적으로 트래픽 암호화 키를 분배받지 못한 가입자 단말들은 다음 주기의 트래픽 암호화 키를 기지국으로 요구한다(S285). 따라서 가입자 단말은 최초 트래픽 암호화 키 분배 절차와 동일하게 Key Request 메시지와 Key Reply 메시지를 Primary Management Connection을 통해 기지국과 교환함으로써 트래픽 암호화 키 갱신을 완료하게 된다(S285, S290). 이 후, x 번째 트래픽 암호화 키의 유효 시간이 만료되면 해당 x+1 번째의 트래픽 암호화 키의 실제 유효 시간이 시작된다(S295). 이후부터 제공받은 해당 서비스 데이터는 x+1 번째의 트래픽 암호화 키에 의해 복호화된다.

<119> 도 10은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서 복수의 가입자 단말과 기지국 간의 트래픽 암호화 키 갱신 방법의 흐름도이다.

<120> 도 10에 도시된 가입자 단말(100-1, 100-2, 100-3, …, 100-z)은 하나의 동일한 멀티캐스트 서비스나 브로드캐스트 서비스를 현재 제공받고 있는 단말들이다. 여기서 하나의 멀티캐스트 서비스나 브로드캐스트 서비스가 n 번째 SA와 관련되어 있다고 가정한다.

<121> 이 때, 기지국(200)은 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 자체적으로 갱신하기 위해서 내부적으로 도 7에서 언급한 바와 같이 M&B TEK Grace Time을 관리하고 있는데, 이 M&B TEK Grace Time 시점에 M&B TEK Refresh Timeout 이벤트가 발생한다.

<122> 이러한 M&B TEK Refresh Timeout 이벤트 발생으로 인해 기지국(200)은 해당 서비스용 트래픽 암호화 키를 자동으로 갱신하고 이를 모든 가입자 단말(100-1,

100-2, 100-3, …, 100-z)들에게 하나의 Key Reply 메시지를 브로드캐스트 커넥션을 통해 전송함으로써 트래픽 암호화 키를 분배한다(S250-1, S250-2, S250-3, …, S250-z). 이 때 기지국에서 전송하는 Key Reply 메시지의 MAC 헤더에는 모든 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 한번에 전달할 수 있는 브로드캐스트 CID가 사용된다.

<123> 따라서, 본 발명의 제1 실시예에 따른 방식에서 기지국(200)이 특정 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 갱신하여 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 분배하기 위해서 무선 채널 구간에서 사용하는 신호 자원은 총 55바이트에 불과하다. 이에 비해, 종래 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키 갱신을 시작하는 방식에서는 z개의 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 트래픽 암호화 키를 갱신하는데 총 110 × z 바이트의 신호 자원이 필요하므로 본 발명의 실시예에 따른 방식이 매우 효율적임을 알 수 있다. 또한, 기지국(200) 입장에서 볼 때, 종래 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 트래픽 암호화 키 갱신을 시작하는 방식에서는 한 순간에 MAC 메시지와 해당 SA를 생성하는데 너무나 많은 처리량이 필요하지만, 본 발명의 실시예에 따른 방식에서는 작은 처리량으로도 해당 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받고 있는 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 트래픽 암호화 키를 안정적으로 갱신 및 분배할 수 있다는 장점이 있다.

<124> 도 11은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래

픽 암호화 키 관리 방법에 따라 트래픽 암호화 키 분배시 MAC 헤더의 CID값과 이에 따른 트래픽 암호화 키를 암호화하는 입력 키간의 관계를 설명해 주는 테이블이다.

<125> 본 발명의 실시예에서는 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 가입자 단말(100)이 분배받을 때에 있어서 두 가지 과정으로 정의할 수 있다. 하나는 가입자 단말(100)이 임의의 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받기 위해 해당 서비스용 트래픽 암호화 키 분배를 요청하는 과정과 또 다른 하나는 그 후 기지국(200)이 해당 서비스를 제공받고 있는 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 일률적으로 해당 트래픽 암호화 키를 갱신하여 분배하는 과정이 있다.

<126> 이 때 기지국(200)에서 분배하는 트래픽 암호화 키는 입력키를 사용하는 3-DES(Data Encryption Standard) 방식이나 AES(Advanced Encryption Standard) 방식의 알고리즘을 이용하여 암호화되어 가입자 단말(100)에게 전달된다.

<127> 한편, 암호화된 트래픽 암호화 키를 수신한 가입자 단말(100)은 미리 공유한 두 개의 입력키를 사용하여 복호해서 실제적인 트래픽 암호화 키를 갖게 되는 것이다. 트래픽 암호화 키의 지속적인 보안을 유지하기 위해서 가입자 단말(100)의 요청에 따른 트래픽 암호화 키 갱신 과정과 기지국(200)의 자체적인 트래픽 암호화 키 갱신 과정에 따라 트래픽 암호화 키를 암호화하는데 사용되어지는 입력키들이 달라진다.

<128> 먼저, 가입자 단말(100)이 해당 서비스의 트래픽 암호화 키에 대한 분배를 요청할 때에는 가입자 단말(100)이 Key Request 메시지를 기지국(200)으로 전송하

고, 기지국(200)은 이에 대한 응답 메시지로써 갱신된 트래픽 암호화 키를 포함한 Key Reply 메시지를 가입자 단말(100)로 전송한다. 이 경우 Key Request 메시지와 Key Reply 메시지는 기지국(200)과 하나의 가입자 단말(100)과의 교환을 하기 때문에 MAC 헤더의 CID 값에 Primary Management CID를 사용한다. 즉, 가입자 단말(100)의 사유 채널인 Primary Management Connection을 통해 수신 받은 트래픽 암호화 키는 해당 가입자 단말(100)과 기지국(200)만이 알고 있는 사유키(Private Key)를 통해 암호화되어 있다. 이 때 사유키는 해당 가입자 단말(100)의 인증키(AK)로부터 만들어진 KEK(Key Encryption Key)를 사용한다. 128비트인 KEK가 Primary Management CID를 사용하여 분배되는 트래픽 암호화 키를 3-DES 방식 또는 AES 방식의 알고리즘으로 암호화하는데 있어서 입력키가 되는 것이다.

<129> 다음, 기지국(200)이 자체적으로 트래픽 암호화 키를 갱신하고 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 일률적으로 분배하는 과정에 있어서 Key Reply 메시지를 이용하여 트래픽 암호화 키를 전송한다. 이 경우 Key Reply 메시지는 기지국(200)에서 해당 서비스를 제공 받고 있는 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 전송되야 하기 때문에 MAC 헤더의 CID값에 Broadcast CID를 사용한다. 해당 서비스의 트래픽 암호화 키를 Broadcast Connection을 통해 전송하기 때문에 기지국(200)과 단말(100-1, 100-2, 100-3, …, 100-z) 사이의 동일한 사유키를 가지고 이 트래픽 암호화 키를 암호화할 수 없다. 그러므로, 이 경우에 있어서 사유키를 사용하지 않고 기지국(200)과 해당 서비스를 제공받고 있는 모든 가입자 단말(100-1, 100-2, 100-3, …, 100-z) 사이의 공용키를 가지고 트래픽 암

호화 키를 암호화하여 분배해야 한다. 하지만, 이 공용키는 멀티캐스트 서비스마다 또한 브로드캐스트 서비스에서만 고유하고 보안을 유지할 수 있는 키이어야 한다. 해당 서비스 트래픽 데이터 암호용으로 사용하였던 이전에 분배받았던 트래픽 암호화 키(Old distributed TEK)는 이러한 특성을 가지고 있는 공용키이다. 멀티캐스트 서비스마다 또한 브로드캐스트 서비스에서만 개별적인 이전에 분배받았던 64비트의 트래픽 암호화 키가 Broadcast CID를 사용하여 분배되는 트래픽 암호화 키를 3-DES 방식이나 AES 방식의 알고리즘으로 암호화하는데 있어서 입력키가 된다. 3-DES 방식에서 두 개의 입력키는 이전에 분배받았던 64비트의 트래픽 암호화 키가 두 번 사용되는 것이고, AES 방식에서의 입력키는 이전에 분배받았던 64비트의 트래픽 암호화 키를 두 번 연결하여 사용되는 것이다.

<130> 따라서, 기지국(200)은 가입자 단말(100)의 요청으로 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키 갱신 및 분배할 때 갱신된 트래픽 암호화 키는 KEK를 입력으로 하여 암호화하고 이를 Primary Management CID를 사용하여 가입자 단말(100)에게 전송하며, 기지국(200) 자체적으로 해당 서비스용 트래픽 암호화 키 갱신 및 분배할 때에는 갱신된 트래픽 암호화 키는 이전에 해당 서비스용으로 생성하였던 트래픽 암호화 키를 입력으로 하여 암호화하여 이를 Broacast CID를 사용하여 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 전송한다. 또한, 가입자 단말(100)은 Primary Management CID를 사용한 Key Reply 메시지를 통해 트래픽 암호화 키를 전달받았다면 KEK를 이용하여 트래픽 암호화 키를 복호하고, Broadcast CID를 사용한 Key Reply 메시지를 통해 트래픽 암호화 키를 전달받았다

면 해당 서비스용으로 이전에 분배받았던 트래픽 암호화 키(Old distributed TEK)를 이용하여 트래픽 암호화 키를 복호하는 것이다.

<131> 이로써, 트래픽 암호화 키조차도 계속적으로 보안을 유지하고 기지국(200)으로부터 Broadcast Connection을 통해 자동으로 갱신된 트래픽 암호화 키를 분배받음으로써 시스템 전체적으로 효율적으로 운영할 수 있다.

<132> 이하, 첨부된 도면을 참조하여 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에 대해서 상세하게 설명한다.

<133> 도 12는 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법의 흐름도이다.

<134> 도 12를 참조하면, 먼저 가입자 단말(100)이 임의의 멀티캐스트 서비스나 브로드캐스트 서비스를 실질적으로 제공받기 전에 우선 해당 서비스 트래픽 데이터를 복호하는데 필요한 트래픽 암호화 키를 분배받아야 한다. 이와 같이 가입자 단말(100)이 기지국(200)으로부터 최초로 해당 서비스의 트래픽 암호화 키를 분배받는 과정(S300, S310)은 도 5를 참조하여 설명한 가입자 단말(100)의 최초 트래픽 암호화 키 요청 및 분배 과정(S100, S110)과 동일하므로 여기에서는 상세한 설명을 생략한다. 그러나, 이 때 기지국(200)으로부터 가입자 단말(100)로 전송되는 Key Reply 메시지에는 트래픽 암호화 키를 암호화하기 위해서 필요한 GKEK(Group Key Encryption Key)가 포함되어 있다. 여기서 GKEK는 가입자 단말(100)과 기지국(200)이 미리 공유한 가입자 단말(100)의 인증키로 암호화되어 있는 키로 멀티캐스트 서비스나 브로드캐스트 서비스에서만 정의되는 파라미터이다.

<135> 이와 같이, 가입자 단말(100)이 기지국(200)으로부터 n 번째 SA에 대해 x 번째로 생성한 해당 서비스의 트래픽 암호화 키가 포함된 Key Reply 메시지를 수신받은 때부터 단말(100)의 x 번째의 트래픽 암호화 키의 실제 유효 시간이 시작되고(S320), 이 유효 시간동안 가입자 단말(100)은 해당 서비스를 제공받을 때 x 번째 트래픽 암호화 키를 가지고 트래픽 데이터를 복호하여 사용한다.

<136> 한편, 해당 서비스의 트래픽 데이터를 끊임없이 안전하게 기지국이 가입자 단말에게 제공하기 위해서 n 번째 SA의 트래픽 암호화 키를 주기적으로 갱신해야 한다.

<137> 그러나, 본 발명의 제2 실시예에서도 도 5를 참조하여 설명한 바와 같이 일반적인 무선 휴대 인터넷 시스템에서처럼 가입자 단말(100)이 TEK Grace time에 의한 트래픽 암호화 키 갱신을 유발하지 않고, 기지국(200)이 해당 서비스 트래픽 암호화 키를 주기적으로 갱신하는 것은 도 8 내지 도 11을 참조하여 설명한 제1 실시예와 유사하지만, 본 발명의 제2 실시예에서는 제1 실시예에서 도 8을 참조하여 설명한 바와 같이 무조건 M&B TEK Grace Time의 시작으로 인해 기지국(200)이 트래픽 암호화 키 갱신을 자동으로 유발하지 않고, M&B TEK Grace Time의 시작 전후로 두 종류의 키 갱신 명령인 Key Update Command 메시지를 사용하여 키 갱신을 수행한다. 이 때, 본 발명의 제2 실시예에서는 제1 실시예에서와 마찬가지로 기지국(200)이 도 7을 참조하여 설명한 바와 같은 M&B TEK Grace Time 파라미터를 관리하고 있다.

<138> 따라서, 본 발명의 제2 실시예에서는 멀티캐스트 서비스나 브로드캐스트 서

비스별로 이 M&B TEK Grace Time이 시작되기 전에 해당 서비스를 제공받고 있는 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 개별적으로 첫 번째 Key Update Command 메시지를 전송한다(S330). 이러한 메시지를 통해서 기지국(200)은 해당 서비스를 제공받는 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 다음 트래픽 암호화 키를 암호화하는데 필요한 20 바이트의 GKEK를 분배한다.

<139> 한편, 기지국(200)은 GKEK를 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 분배할 때 한 시점에 집중되지 않도록 하기 위해서 기지국 내부적으로 첫 번째 Key Update Command 메시지를 시간적으로 분산시켜 개별적으로 전송한다.

<140> 따라서, 상기 단계(S330)에서 기지국(200)에서 가입자 단말(100-1, 100-2, 100-3, …, 100-z)로 전송되는 Key Update Command 메시지의 MAC 헤더에는 개별적인 가입자 단말을 나타내기 위해 Primary Management CID가 사용되고, GKEK는 해당 가입자 단말(100-1, 100-2, 100-3, …, 100-z)과 공유하고 있는 인증키인 AK를 사용하여 암호화되어 전송된다. 이 후, 멀티캐스트 서비스나 브로드캐스트 서비스별로 이 M&B TEK Grace Time 시점이 되면(S340) 기지국(200)은 M&B TEK Refresh Timeout 이벤트를 발생시킨다(S350). 여기에서도 마찬가지로, 기지국(200) 내부에는 이러한 M&B TEK Refresh Timeout 이벤트를 수행할 트래픽 암호화 키 상태 머신이 소프트웨어로 구현되어 있다.

<141> 따라서, 기지국(200)은 이러한 M&B TEK Refresh Timeout 이벤트로 인해 트래픽 암호화 키 상태 머신을 통해 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 새롭게 갱신하게 된다. 이 때 갱신되는 트래픽 암호화 키는 x+1

번째 트래픽 암호화 키가 된다.

<142> 그 후, 기지국(200)은 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 n 번째 SA에 대해 갱신된 x+1 번째 트래픽 암호화 키를 포함하는 두 번째 Key Update Command 메시지를 한 번에 방송적으로 전송한다(S360). 즉, 상기 단계(S360)에서 가입자 단말(100-1, 100-2, 100-3, …, 100-z)로 전송되는 Key Update Command 메시지는 Broadcast Connection을 통해 전송되며, 이 메시지의 MAC 헤더에는 Broadcast CID가 사용된다. 이 때 전송되는 트래픽 암호화 키는 전에 할당받은 GKEK로 암호화되어 전송된다.

<143> 이와 같이, GKEK와 트래픽 암호화 키를 포함한 두 개의 Key Update Command 메시지를 모두 수신한 가입자 단말(100)에서는 내부적으로 관리하고 있는 TEK Grace Time이 동작하지 않게 된다.

<144> 이 후, x 번째 트래픽 암호화 키의 유효 시간이 만료되면 해당 x+1 번째의 트래픽 암호화 키의 실제 유효 시간이 시작된다(S370). 이 후부터 가입자 단말(100)과 기지국(200)은 제공받은 해당 서비스 데이터에 대해 x+1 번째의 트래픽 암호화 키를 가지고 복호화하는 것이다.

<145> 본 발명의 제2 실시예에서 제안하는 멀티캐스트 서비스나 브로드캐스트 서비스에 대한 트래픽 암호화 키를 갱신하기 위해서 Key Update Command 라는 메시지를 두 번 사용한다. 처음은 다음 유효 시간 동안 사용될 트래픽 암호화 키를 암호화하는데 사용될 GKEK를 분배하기 위한 것으로, 기지국(200)은 M&B TEK Grace Time 시간 이전에 해당 서비스를 제공받고 있는 모든 단말(100-1, 100-2, 100-3, …,

100-z)에게 개별적으로 Primary Management Connection을 통해 각각 전송한다. 이 때의 Key Update Command 메시지는 최대 50바이트 크기를 가진다. 다음에는 기지국(200)이 내부적으로 관리하고 있는 타이머인 M&B TEK Grace Time 시점에 기지국(200)이 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 다음 유효 시간동안 사용될 트래픽 암호화 키를 한 번의 Key Update Command 메시지를 브로드캐스트 커넥션을 통해 방송적으로 분배한다. 이 때 트래픽 암호화 키가 포함된 Key Update Command 메시지는 최대 50바이트 크기를 가진다.

<146> 도 13은 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서 복수의 가입자 단말과 기지국 간의 트래픽 암호화 키 갱신 방법의 흐름도이다.

<147> 도 13에 도시된 가입자 단말(100-1, 100-2, 100-3, …, 100-z)은 하나의 동일한 멀티캐스트 서비스나 브로드캐스트 서비스를 현재 제공받고 있는 단말들이다. 여기서 하나의 멀티캐스트 서비스나 브로드캐스트 서비스가 n 번째 SA와 관련되어 있다고 가정한다.

<148> 이 때, 기지국(200)은 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 자체적으로 갱신하기 위해서 내부적으로 도 7에서 언급한 바와 같이 M&B TEK Grace Time을 관리하고 있는데, 이 M&B TEK Grace Time 시점 이전에 기지국(200)은 모든 가입자 단말(100-1, 100-2, 100-3, …, 100-z) 각각에게 Primary Management Connection을 통해 첫 번째 Key Update Command를 전송하여 다음 트래픽 암호화 키를 암호하는데 필요한 GKEK를 분배한다(S330-1, S330-2, S330-3, …, S330-z). 이 때, 기지국(200)은 GKEK를 분배하기 위해서 Key Update Command 메시

지를 일정 시간에 걸쳐 기지국(200)에 부하가 생기지 않도록 하나씩 전송한다. 따라서, 이 때 전송되는 Key Update Command 메시지의 MAC 헤더에는 Primary Management CID가 사용된다.

<149> 이 후, M&B TEK Grace Time 시점이 되면, 기지국(200)에서 M&B TEK Refresh Timeout 이벤트가 발생한다. 이러한 M&B TEK Refresh Timeout 이벤트 발생으로 인해 기지국(200)은 해당 서비스용 트래픽 암호화 키를 자동으로 갱신하고 이를 모든 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 두 번째 Key Update Command 메시지를 Broadcast Connection을 통해 전송함으로써 트래픽 암호화 키를 분배한다(S360-1, S360-2, S360-3, …, S360-z). 이 때 기지국(200)에서 전송하는 Key Update Command 메시지의 MAC 헤더에는 모든 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 한번에 전달할 수 있는 Broadcast CID가 사용된다.

<150> 따라서, 본 발명의 제2 실시예에 따른 방식에서 기지국(200)이 특정 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 갱신하여 z개의 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 분배하기 위해서 무선 채널 구간에서 사용하는 첫 번째 Key Update Command 메시지는 총 50×z 바이트이고, 두 번째 Key Update Command 메시지는 50 바이트가 된다. 즉, 사용되는 신호 자원은 총 (50×z + 50) 바이트에 불과하다. 이에 비해, 종래 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키 갱신을 시작하는 방식에서는 z개의 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 트래픽 암호화 키를 갱신하는데 총 110 × z 바이트의 신호 자원이 필요하다. 이는

해당 멀티캐스트 서비스나 브로드 캐스트 서비스를 제공받는 단말이 많아질수록 본 발명의 제2 실시예에 따른 방식이 매우 효율적임을 보여준다. 또한, 기지국(200) 입장에서 볼 때, 종래 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 트래픽 암호화 키 갱신을 시작하는 방식에서는 통해 한 순간에 MAC 메시지와 해당 SA를 생성하는데 너무나 많은 처리량이 필요하지만, 본 발명의 제2 실시예에 따른 방식에서는 로드 분산을 통해 작은 처리량으로도 해당 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받고 있는 가입자 단말(100-1, 100-2, 100-3, …, 100-z)에게 트래픽 암호화 키를 안정적으로 갱신 및 분배할 수 있다는 장점이 있다.

<151> 도 14는 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에서 사용되는 트래픽 암호화 키 응답(Key Reply) 메시지의 내부 파라미터들을 나타낸 테이블을 도시한 도면이다.

<152> 도 12에 도시된 단계(S300, S310)에서 가입자 단말(100)이 멀티캐스트 서비스나 브로드캐스트 서비스에 대한 최초 트래픽 암호화 키 요청 시에 이에 대한 응답 메시지로 기지국(200)은 Key Reply 메시지를 가입자 단말(100)로 전송한다(S310). 이 때 Key Reply 메시지에는 도 14에 도시된 바와 같이 트래픽 암호화 키와 관련된 인증키 일련 번호를 의미하는 Key-Sequence-Number, 해당 SA의 식별자인 SA-ID, 현재의 트래픽 암호화 키 유효 시간과 다음의 트래픽 암호화 키 유효 시간 동안 유효한 트래픽 암호화 키와 관련된 파라미터들인 TEK-Parameters과 이 Key Reply 메시지 인증 기능을 위한 HMAC-Digest가 포함된다.

<153> 도 15는 도 14에 도시된 트래픽 암호화 키 관련 파라미터(TEK-Parameters)를

을 표현한 테이블을 도시한 도면이다.

<154> 도 15를 참조하면 트래픽 암호화 키 관련 파라미터(TEK-Parameters)에는 GKEK가 포함된다. 이 GKEK는 멀티캐스트 서비스나 브로드캐스트 서비스에서만 정의되는 파라미터로써 그룹 키 암호화 키(Group Key Encryption Key)로써, 랜덤하게 생성되어 트래픽 암호화 키를 암호하는데 필요한 키이고, 이 GKEK도 가입자 단말(100)에게 분배한 인증키(AK)로 암호화되어서 전송된다.

<155> 또한, 트래픽 암호화 키(TEK)도 트래픽 암호화 키 관련 파라미터(TEK-Parameters)에 포함되며, 트래픽 데이터를 암호화하는데 필요한 입력 키이다. 기지국(200)이 트래픽 암호화 키를 해당 서비스를 제공받고 있는 가입자 단말(100)에게 안전하게 전송하기 위해서 트래픽 암호화 키 자체도 암호화해서 전송하며, 이때 사용되는 키가 GKEK이다. 반면에, 유니캐스트 서비스용 트래픽 암호화 키나 본 발명의 제1 실시예에서의 트래픽 암호화 키는 KEK로 암호화된다.

<156> 이외에 트래픽 암호화 키 관련 파라미터(TEK-Parameters)에는 트래픽 암호화 키 유효 시간(Key-Lifetime), 트래픽 암호화 키 일련 번호(Key-Sequence-Number), 트래픽 데이터를 암호화하는데 필요한 입력 키 역할을 하는 CBC(Cipher Block Chaining)-IV(Initialization Vector)가 포함된다.

<157> 특히, 멀티캐스트 서비스와 브로드캐스트 서비스에 있어서 유니캐스트 서비스와 달리 GKEK와 트래픽 암호화 키는 멀티캐스트 서비스마다 그리고 브로드캐스트 서비스마다 동일하다. 즉, 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받고 있는 모든 단말(100-1, 100-2, 100-3, …, 100-z)은 동일한 GKEK와 트래픽 암호화

키를 공유하는 것이다. 이 때의 GKEK와 트래픽 암호화 키는 기지국(200) 또는 인증 서버(AAA)에서 랜덤하게 생성된다. 그 기준은 이러한 서비스를 관리하는 범위에 따라 다른데, 그 범위가 단일 기지국일 경우에는 기지국(200)이 GKEK와 트래픽 암호화 키를 생성하고, 이와 반대로 망 전체적인 경우에는 인증 서버(AAA)가 이 키들을 생성한다. 또한, GKEK의 일련번호와 유효 시간은 트래픽 암호화 키의 일련번호화 유효 시간과 동일하게 적용된다.

<158> 도 16은 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에서 사용되는 키 갱신 명령(Key Update Command) 메시지의 내부 파라미터들을 나타낸 테이블을 도시한 도면이다.

<159> 도 16을 참조하면, 이 Key Update Command 메시지는 멀티캐스트 서비스와 브로드캐스트 서비스에 한해서 정의되는 메시지이고, 다음과 같은 파라미터들을 포함한다.

<160> 먼저, Key Update Command 메시지를 통해 새로이 분배할 트래픽 암호화 키(TEK)와 관련된 인증키 일련 번호를 의미하는 Key-Sequence-Number와 해당 SA의 식별자인 SA-ID가 포함된다.

<161> 또한, Key Update Command 메시지는 도 12에 도시된 바와 같이 두 종류가 존재하며, 이를 구별해주기 위한 코드인 키 푸시 모드(Key Push Modes)가 포함된다.

<162> 또한, Key Update Command 메시지 자체의 인증을 위하여 HMAC-Digest가 사용되는데, 이 때 리플레이 공격(Replay Attack) 방지하기 위해 키 푸시 카운터(Key Push Counter)가 포함된다. 이 키 푸시 카운터는 기지국(200)이 해당 멀티캐스트

서비스나 브로드캐스트 서비스마다 관리하는 파라미터로 이 Key Update Command 메시지를 송신할 때마다 1씩 증가시킨 2바이트인 파라미터이다.

<163> 또한, 도 15에서 정의된 TEK-Parameters들이 포함되어 있으며, 인증 기능을 위한 HMAC-Digest도 포함된다.

<164> 특히, GKEK를 갱신하기 위해서 해당 서비스를 제공받고 있는 모든 단말(100-1, 100-2, 100-3, …, 100-z) 각각에게 전송하는 첫 번째 Key Update Command 메시지와 트래픽 암호화 키를 갱신하기 위해서 해당 서비스를 제공받고 있는 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 브로드캐스트 커넥션을 통해 동시에 전송하는 두 번째 Key Update Command 메시지에 포함되는 파라미터들은 각각 다르다.

<165> 즉, 첫 번째와 두 번째 Key Update Command 메시지에는 TEK-Parameters를 제외한 인증키용 Key-Sequence-Number와 SA-ID와 Key Push Modes와 Key Push Counter 그리고 HMAC-Digest는 공통으로 포함되어 있다. 그러나, TEK-Parameters에 포함되어 있는 부파라미터들 중에서 GKEK와 트래픽 암호화 키용 Key-Sequence-Number는 첫 번째 Key Update Command 메시지에 포함되고, 트래픽 암호화 키(TEK)와 트래픽 암호화 키 유효 시간(Key-Lifetime)과 트래픽 암호화 키 일련 번호(Key-Sequence-Number) 그리고 CBC-IV는 두 번째 Key Update Command 메시지에 포함된다.

<166> 도 17은 도 16에 도시된 Key push modes 파라미터를 표현한 테이블을 도시한 도면이다.

<167> 이 Key push modes는 Key Update Command 메시지의 용도를 구별해주는 코드이다. 멀티캐스트 서비스나 브로드캐스트 서비스에 대한 트래픽 암호화 키를 갱신

하는데 있어서 기지국(200)은 두 번의 Key Update Command 메시지를 가입자 단말(100)로 전송한다. 첫 번째 Key Update Command 메시지는 GKEK를 갱신하기 위해 사용되고, 두 번째 Key Update Command 메시지는 실질적인 트래픽 암호화 키를 갱신하여 가입자 단말(100)로 분배하기 위해 사용된다. 따라서, 이 Key push modes에 따라 Key Update Command 메시지의 용도가 나타나며, 도 17을 참조하면 그 값이 0인 경우에는 GKEK를 갱신하기 위한 첫 번째 Key Update Command 용도인 것을 나타내고, 그 값이 1인 경우에는 트래픽 암호화 키를 갱신하기 위한 두 번째 Key Update Command 용도인 것을 나타낸다. 따라서 가입자 단말(100)에서는 이러한 Key push modes 파라미터 값을 보고 그 용도를 알 수 있다.

<168> 도 18은 도 16에 도시된 HMAC-Digest 파라미터를 생성할 때 사용되는 입력키를 표현한 테이블을 도시한 도면이다.

<169> 본 발명의 제2 실시예에서 사용되는 Key Update Command 메시지 자체를 인증하기 위해서 HMAC-Digest가 필요한데, 하향 링크 메시지인 Key Update Command 메시지의 HMAC 인증 키(HMAC authentication key)들을 생성 시 사용되는 입력키는 Key Update Command 메시지에 따라 즉, Key push modes에 따라 다르다.

<170> 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받는 모든 가입자 단말 각각에게 따로 전송하는 첫 번째 Key Update Command 메시지, 즉 Key push modes가 GKEK 갱신 모드일 때 HMAC 인증 키를 만드는 입력 키는 해당 가입자 단말에게 미리 분배한 인증키(AK)이다. 이와는 달리, 위 서비스를 제공받는 모든 단말에게 동시에 전송하는 두 번째 Key Update Command 메시지, 즉 Key push modes가 TEK 갱신

모드일 때 HMAC 인증 키를 생성하는데 필요한 입력 키는 GKEK 갱신 모드의 Key Update Command 메시지를 통해 분배한 GKEK이다. TEK 갱신 모드의 Key Update Command 메시지는 방송적으로 전송하기 때문에, 서비스를 제공받고 있는 모든 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 이 메시지를 인증할 수 있어야 한다. 따라서, 기지국(200) 뿐만 아니라 해당 서비스를 제공받고 있는 모든 가입자 단말(100-1, 100-2, 100-3, …, 100-z)이 안전하게 공유하고 있는 키는 GKEK이기 때문이다.

<171> 또한, 이 HMAC 인증 키에 사용되는 또 다른 입력키로 키 푸시 카운터가 사용되는데, 이 키 푸시 카운터는 매 키 갱신 명령 메시지마다 1씩 증가시킴으로써 이 키 갱신 명령 메시지에 대한 리플레이 공격을 방지하도록 한다.

<172> 각각의 키 갱신 명령 메시지 인증을 위해 사용되는 하향 링크 HMAC 인증 키를 생성하는 한 가지 방법으로 다음과 같은 예를 들 수 있다.

<173> HMAC_KEY_D = SHA(H_PAD_D|KeyIN|Key Push Counter)

<174> with H_PAD_D = 0x3A repeated 64 times.

<175> 하향 링크 HMAC 인증 키는 SHA(Secure Hash Algorithm) 방식을 사용하여 생성한다. 여기서, SHA는 미국 NIST에 의해 개발된 SHS(Secure Hash Standard) 내에 정의된 알고리즘이다. 상기 하향 링크 HMAC 인증 키를 생성하는데 있어서, 0x3A 값이 64바이트만큼 반복된 값을 가지는 H_PAD_D, KeyIN와 Key Push Counter가 서로 연결되어 입력된다. 여기서 KeyIN은 제1 키 갱신 명령 메시지에서는 가입자 단말의 인증키이고, 제2 키 갱신 명령 메시지에서는 상기 멀티캐스트 서비스별 또는 브

로드캐스트 서비스별마다 관리하고 있는 GKEK이다.

<176> 한편, 도 12에 도시된 바와 같이 기지국(200)이 두 번의 Key Update Command 메시지를 통해 트래픽 암호화 키를 자동으로 갱신하여 가입자 단말(100)로 분배하는 과정에서, 가입자 단말(100)이 두 종류의 Key Update Command 메시지를 올바르게 수신하지 못하였을 경우에 대해 도 19를 참조하여 설명한다.

<177> 도 19를 참조하면, 가입자 단말(100)이 기지국(200)으로부터 최초로 해당 서비스의 트래픽 암호화 키를 분배받는 과정(S300, S310)부터 기지국(200)이 내부의 M&B TEK Grace Time 시점을 기준으로 GKEK 갱신 모드의 첫 번째 Key Update Command 메시지와 TEK 갱신 모드의 두 번째 Key Update Command 메시지를 해당 서비스를 제공받고 있는 단말(100)에게 전송하는 과정(S360)까지는 동일하게 진행된다.

<178> 그러나, 이러한 과정에서 가입자 단말(100)이 기지국(200)에서 전송된 두 번의 Key Update Command 메시지 중 하나의 메시지라도 정상적으로 수신하지 못하였을 경우, 즉 비정상적으로 트래픽 암호화 키를 분배받지 못하였을 경우, 해당 단말(100)은 도 1을 참조하여 설명한 바와 같이 가입자 단말(100)이 개별적으로 트래픽 암호화 키를 갱신 요청하여 기지국(200)으로부터 분배받는 과정을 거친다. 즉, 비정상적으로 트래픽 암호화 키를 분배받지 못한 가입자 단말(100)에서는 내부적으로 관리하고 있는 TEK Grace Time이 동작하게 되고(S380), 가입자 단말(100) 내부에 있는 트래픽 암호화 키 상태 머신에서 TEK Refresh Timeout 이벤트가 발생한다(S390). 이러한 이벤트 발생으로 인해 가입자 단말(100)은 다음 주기의 트래픽 암

호화 키를 기지국(200)으로 요구한다(S400). 따라서 가입자 단말(100)은 최초 트래픽 암호화 키 분배 절차와 동일하게 Key Request 메시지와 Key Reply 메시지를 Primary Management Connection을 통해 기지국과 교환함으로써 트래픽 암호화 키 갱신을 완료하게 된다(S400, S410). 이 후, x 번째 트래픽 암호화 키의 유효 시간이 만료되면 해당 x+1 번째의 트래픽 암호화 키의 실제 유효 시간이 시작된다(S420). 이 후부터 제공받은 해당 서비스 데이터는 x+1 번째의 트래픽 암호화 키에 의해 복호화된다.

<179> 도 20은 도 19에 도시된 제2 실시예에서 비정상적인 경우의 트래픽 암호화 키 관리 방법에서 가입자 단말의 트래픽 암호화 키 요청 상황에 따른 Key Reply 메시지에 포함되어 전송되는 TEK-Parameters 정보를 나타내는 테이블이다.

<180> 도 19를 참조하면, 가입자 단말(100)은 여러 시점에서 트래픽 암호화 키 요청 메시지인 Key Request 메시지를 기지국(200)으로 전송할 수 있다.

<181> 먼저, 가입자 단말(100)이 임의의 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받기 위해서 어느 시점에서든지 Key Request 메시지를 통해 트래픽 암호화 키를 최초로 요구할 수 있다. 이와 같은 Key Request 메시지를 수신받은 기지국(200)은 내부적으로 관리하고 있는 M&B TEK Grace Time 시점을 기준으로 가입자 단말(100)로 전송하는 트래픽 암호화 키 응답 메시지인 Key Reply 메시지의 내부 파라미터들을 다르게 구성한다.

<182> 예를 들어, 도 19를 참조하면 기지국(200)이 M&B TEK Grace Time 시작 시점(ⓐ) 이전에 가입자 단말(100)로부터 최초로 트래픽 암호화 키를 요구하는 Key

Request 메시지를 수신받은 경우(Initial TEK response)에는 해당 서비스의 현재 주기 동안 유효한 TEK-Parameters가 포함된 Key Reply 메시지를 가입자 단말(100)로 전송한다.

<183> 이와 달리 기지국(200)이 M&B TEK Grace Time 시작 시점(ⓐ) 이후에 가입자 단말(100)로부터 최초로 트래픽 암호화 키를 요구하는 Key Request 메시지를 수신받은 경우(Initial TEK response)에는 해당 서비스의 현재 주기 동안 유효한 TEK-Parameters (TEK-Parameters$_C$)와 다음 주기 동안 유효한 TEK-Parameters (TEK-Parameters$_N$)가 모두 포함된 Key Reply 메시지를 가입자 단말(200)로 전송한다. 이는 모든 단말(100-1, 100-2, 100-3, …, 100-z)에게 다음 주기 동안 유효한 트래픽 암호화 키를 공개하는 시점(ⓐ) 이전에 기지국(200)이 어떠한 단말(100-1, 100-2, 100-3, …, 100-z)에게도 다음 주기 동안 유효한 트래픽 암호화 키 관련 파라미터인 TEK-Parameters (TEK-Parameters$_N$) 정보를 주지 않는 장점뿐만 아니라, 트래픽 암호화 키 응답 메시지인 Key Reply 메시지의 양도 줄일 수 있다는 장점이 있다.

<184> 또한, 해당 서비스를 제공받고 있는 단말(100-1, 100-2, 100-3, …, 100-z)에게 다음 주기 동안 유효한 트래픽 암호화 키를 공개한 시점(ⓐ) 이후에 기지국(200)은 트래픽 암호화 키를 요구한 단말(100-1, 100-2, 100-3, …, 100-z)에게 현재뿐만 아니라 다음 주기 동안 유효한 TEK-Parameters (TEK-Parameters$_N$)를 전송함으로써 단말(100)이 관리하고 있는 TEK Grace Time 시작 시점(ⓑ) 이후에 다음 주기 동안 유효한 트래픽 암호화 키 요청을 하지 않도록 하기 위함이다.

<185> 만약, TEK Grace Time 시작 시점(ⓑ) 이후에 가입자 단말(100)이 새로운 트래픽 암호화 키를 요청하게 되면, 이러한 요청은 트래픽 암호화 키를 갱신하기 위한 요청(TEK update response)이므로, 기지국(200)은 다음 주기 동안 유효한 TEK-Parameters (TEK-Parameters$_N$)만이 포함된 Key Reply 메시지를 가입자 단말(100)로 전송한다. 이는 가입자 단말(100)은 해당 서비스를 현재 받고 있기 때문에 현재 주기 동안 유효한 TEK-Parameters (TEK-Parameters$_C$)를 이미 가지고 있다고 가정하는 것이다. 이로써, 트래픽 암호화 키 응답 메시지인 Key Reply 메시지 송신시 불필요한 정보들을 줄일 수 있다는 장점이 있다.

<186> 도 21은 본 발명의 제1 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법에서 가입자 단말(100)이 내부적으로 관리하고 있는 트래픽 암호화 키 상태 머신의 상태 천이도이고, 도 22는 도 21에 도시된 상태 천이를 정리하여 나타낸 테이블이다.

<187> 가입자 단말(100)과 기지국(200)은 유니캐스트 서비스, 멀티캐스트 서비스 또는 브로드캐스트 서비스와 상관없이 모든 서비스에 대하여 트래픽 암호화 키 상태 머신 천이도의 흐름을 따르고, 멀티캐스트와 브로드캐스트 서비스별에 대응하여 최대 두 개씩의 트래픽 암호화 키 상태 머신을 포함한다. 이하, 가입자 단말(100)의 위주로 트래픽 암호화 키 상태 머신의 흐름에 대해 설명하지만, 이러한 흐름은 각 이벤트의 발생에 따라 기지국(200)에서 참조할 수 있다.

<188> 먼저, 가입자 단말(100)이 정상 상태로 기동되어 기지국(200)과의 무선 통신

이 가능한 상태가 되면 트래픽 암호화 키 상태 머신은 "Start(시작)" 상태(A)로 시작한다.

<189> 그 후, 도 8에 도시된 바와 같이, 가입자 단말(100)이 멀티캐스트 서비스나 브로드캐스트 서비스를 제공받고자 할 때, 기지국(200)으로 Key Request 메시지를 송신하여 해당 서비스에 대한 트래픽 암호화 키를 요청하여 대기하는 동작 (Authorized, (2))이 발생되면 트래픽 암호화 키 상태 머신은 "Op Wait(동작 대기)" 상태(B)로 천이한다.

<190> 그리고, 가입자 단말(100)이 Key Reply 메시지를 통해 정상적으로 트래픽 암호화 키를 분배받는 동작(Key Reply, (8))이 발생되면 분배받은 트래픽 암호화 키를 기지국(200)과 공유하게 되어 데이터 전송이 가능한 "Operational(동작)" 상태(D)로 천이한다.

<191> 그러나, "Op Wait" 상태(B)에서 기지국(200)으로부터 Key Reject 메시지를 받는 동작(Key Reject, (9))이 발생되면, 다시 "Start" 상태(A)로 천이된다.

<192> 한편, 트래픽 암호화 키 상태 머신이 정상적으로 트래픽 암호화 키를 전달받아서 "Operational" 상태(D)로 대기하는 중에, 일정 시간이 경과하여 가입자 단말(100)이 기지국(200)으로부터 M&B TEK Grace Time 시점에 자동으로 갱신된 트래픽 암호화 키를 Key Reply 메시지를 통해 전달받으면, 내부 트래픽 암호화 키 상태 머신에 Key Reply라는 이벤트(8)를 발생시키고, 이에 따라 트래픽 암호화 키 상태 머신은 기존의 유효한 트래픽 암호화 키를 가지고 있던 "Operational" 상태(D)에서 인증 및 보안과 관련된 자체 데이터베이스에 새로이 갱신된 SA를 저장하고 다시

"Operational" 상태(D)로 머무르게 된다.

<193> 그러나, 도 9에서 설명한 바와 같이 가입자 단말(100)이 "Operational" 상태에서 기지국(200)으로부터 트래픽 암호화 키의 자동 갱신을 위한 Key Reply 메시지와를 제대로 수신하지 못한 경우, TEK Grace Time 시작 시점에 내부 트래픽 암호화 키 상태 머신에 TEK Refresh Timeout라는 이벤트(7)를 발생시키고 "Rekey Wait(갱신 대기)" 상태(E) 상태로 천이시킨다. 이와 동시에, 기지국(200)으로 Key Request 메시지를 통해서 다음 주기 동안 유효한 트래픽 암호화 키를 요청한다.

<194> 그 후, 가입자 단말(100)은 "Rekey Wait" 상태(E)에 있다가 기지국(200)으로부터 트래픽 암호화 키가 포함된 Key Reply 메시지를 받으면, Key Reply 이벤트(8)를 발생시키고 트래픽 암호화 키 상태 머신을 다시 "Operational" 상태(D)로 천이시켜서, 트래픽 암호화 키를 이용한 데이터 전송이 정상적으로 수행될 수 있도록 한다.

<195> 여기에서, "Operational" 상태(D)에서 Key Reply 이벤트(8) 발생에 의해 다시 "Operational" 상태(D)를 유지하는 것은 오직 본 발명의 제1 실시예에 따른 멀티캐스트 서비스나 브로드캐스트 서비스에 한해서만 규정된 것이다.

<196> 상기한 이외에도 트래픽 암호화 키 상태 머신이 위치할 수 있는 상태에는 "Op Reauth Wait" 상태(C) 및 "Rekey Reauth Wait" 상태(F)가 더 있으나, 이들은 종래 수행되던 서비스 때와 동일하게 처리되므로 여기에서는 그 설명을 생략하더라도 본 기술분야의 당업자에 의해 쉽게 이해될 것이다.

<197> 도 23은 본 발명의 제2 실시예에 따른 무선 휴대 인터넷 시스템에서의 트래

픽 암호화 키 관리 방법에서 가입자 단말의 트래픽 암호화 키 상태 머신의 상태 천이도이고, 도 24는 도 23에 도시된 상태 천이를 정리하여 나타낸 테이블이다.

<198> 도 23 및 도 24를 참조하면, 도 21 및 도 22를 참조하여 설명한 본 발명의 제1 실시예의 경우와 유사하므로 여기에서는 본 발명의 제2 실시예에서만 특유한 부분만을 설명하기로 한다.

<199> 가입자 단말(100)의 트래픽 암호화 키 상태 머신이 기지국(200)으로부터 최초로 정상적으로 트래픽 암호화 키를 전달받아서 "Operational" 상태(D)로 대기할 때까지는 동일하다.

<200> 그 후, 트래픽 암호화 키 상태 머신이 "Operational" 상태(D)에 머무르는 중에, 가입자 단말(100)이 기지국(200)으로부터 M&B TEK Grace Time 시점 이전에 GKEK update mode의 Key Update Command 메시지를 전달받으면, 내부 트래픽 암호화 키 상태 머신에 GKEK Updated 라는 이벤트(10)를 발생시키고, 이에 따라 트래픽 암호화 키 상태 머신은 "M&B Rekey Interim Wait(멀티캐스트 또는 브로드캐스트 갱신 잠정 대기" 상태(G)로 천이하여 갱신된 키가 전달되기를 기다린다.

<201> 다음, 기지국(200)은 M&B TEK Grace Time 시점 이후에 TEK update mode의 Key Update Command 메시지를 가입자 단말(100)로 브로드캐스트 커넥션으로 방송하고, 이를 수신한 가입자 단말(100)은 내부 트래픽 암호화 키 상태 머신에 TEK Updated라는 이벤트(11)를 발생시키고 다시 "Operational" 상태(D)로 천이되도록 한다.

<202> 그러나, 도 19에서 설명한 바와 같이 "M&B Rekey Interim Wait" 상태(G)에서

TEK update mode의 Key Update Command 메시지를 제대로 수신받지 못한 가입자 단말(100)은 내부적으로 관리하고 있는 TEK Grace Time 발생 시점에 내부 트래픽 암호화 키 상태 머신에 TEK Refresh Timeout라는 이벤트(7)를 발생시키고 "Rekey Wait" 상태(E)로 천이시킨다. 동시에, 기지국(200)으로 Key Request 메시지를 통해서 다음 주기 동안 유효한 트래픽 암호화 키를 요청한다.

<203> 이와는 달리, 가입자 단말(100)이 "Operational" 상태에서 GKEK update mode의 Key Update Command 메시지를 제대로 수신하지 못한 경우, TEK Grace Time 시점에 내부 트래픽 암호화 키 상태 머신에 TEK Refresh Timeout라는 이벤트(7)를 발생시키고 "Rekey Wait" 상태(E) 상태로 천이시킨다. 마찬가지로, 기지국(200)으로 Key Request 메시지를 통해서 다음 주기 동안 유효한 트래픽 암호화 키를 요청한다.

<204> 다음, 가입자 단말(100)은 앞에서 설명한 두 가지 경우로 인해 "Rekey Wait" 상태(E)에 있다가 기지국(200)으로부터 트래픽 암호화 키가 포함된 Key Reply 메시지를 받으면, Key Reply(8) 이벤트를 발생시키고 트래픽 암호화 키 상태 머신을 다시 "Operational" 상태(D)로 천이시킨다.

<205> 여기에서, "Operational" 상태(D)에서 GKEK Updated 이벤트(10) 발생에 의한 "M&B Rekey Interim Wait" 상태(G)로의 천이와 "M&B Rekey Interim Wait" 상태(G)에서 TEK Refresh Timeout 이벤트(7) 발생에 의한 "Rekey wait" 상태(E)로의 천이 및 TEK Updated 이벤트(11) 발생에 의한 "Operational" 상태(D)로의 천이는 오직 본 발명의 제2 실시예에 따라른 멀티캐스트 서비스나 브로드캐스트 서비스에 한해

서만 규정된 것이다.

<206> 상기한 이외에도 트래픽 암호화 키 상태 머신이 위치할 수 있는 상태에는 "Op Reauth Wait" 상태(C) 및 "Rekey Reauth Wait" 상태(F)가 더 있으나, 이들은 종래 수행되던 서비스 때와 동일하게 처리되므로 여기에서는 그 설명을 생략하더라도 본 기술분야의 당업자에 의해 쉽게 이해될 것이다.

<207> 이상에서 본 발명의 바람직한 실시예에 대하여 상세하게 설명하였지만 본 발명은 이에 한정되는 것은 아니며, 그 외의 다양한 변경이나 변형이 가능하다.

【발명의 효과】

<208> 본 발명은 IEEE 802.16 무선 MAN 시스템과 같은 무선 휴대 인터넷 시스템에서 멀티캐스트 서비스나 브로드캐스트 서비스용 트래픽 암호화 키를 관리하는 방법을 정의하는 것으로, 다음과 같은 효과가 있다.

<209> 첫째, 멀티캐스트 서비스와 브로드캐스트 서비스용 트래픽 암호화 키 갱신을 기지국이 시작하여 갱신된 키를 해당 서비스를 제공받는 가입자 단말들에게 브로드캐스트 커넥션을 통해 전달함으로써, 적은 신호 자원을 가지고도 트래픽 암호화 키의 갱신 및 분배가 가능하다.

<210> 둘째, 기지국이 멀티캐스트 서비스와 브로드캐스트 서비스의 트래픽 암호화 키를 자동으로 갱신하고, 가입자 단말에게 일률적으로 분배하는 방식을 사용함으로써, 가입자 단말로부터 일시적인 트래픽 암호화 키 요청 메시지를 사용하지 않고 한 번의 Key Reply 메시지 또는 두 번의 Key Update Command 메시지로 모든 가입자 단말에게 트래픽 암호화 키를 분배하게 되어 기지국 입장에서 이러한 트래픽 암호

화 키와 관련된 처리량이 감소된다는 장점이 있다.

<211> 셋째, 기지국이 트래픽 암호화 키를 갱신하는데 있어서, 트래픽 암호화 키 자체를 암호화하기 위해 필요한 KEK 또는 GKEK를 단말의 인증키로 암호화해서 모든 단말 각각에게 전송하기 때문에 KEK 또는 GKEK를 안전하게 분배할 수 있다.

<212> 넷째, 트래픽 암호화 키를 모든 가입자 단말에게 브로드캐스트로 전송할지라도 트래픽 암호화 키 자체도 KEK 또는 GKEK로 암호화했기 때문에, 오직 KEK 또는 GKEK를 분배받은 가입자 단말들만 트래픽 암호화 키를 복호할 수 있어서 안전하다라는 장점이 있다.

<213> 다섯째, 멀티캐스트 서비스와 브로드캐스트 서비스용 트래픽 암호화 키를 기지국에서 주기적으로 갱신함으로써 상기 서비스에 대한 강력한 보안을 유지하면서 가입자 단말에게 서비스를 제공할 수 있다.

<214> 여섯째, 멀티캐스트 서비스의 경우 멀티캐스트 서비스마다 관련된 SA 특히 트래픽 암호화 키가 다르므로 멀티캐스트 서비스마다 보안 유지가 가능하다.

<215> 일곱째, 브로드캐스트 서비스의 경우 사업자마다 고유한 SA 특히 트래픽 암호화 키를 관리하므로 타 사업자의 단말들로부터 보안 유지가 되는 서비스를 제공할 수 있다.

【특허청구범위】

【청구항 1】

무선 휴대 인터넷 시스템에서 기지국이 무선 연결된 가입자 단말에 대한 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하는 방법에 있어서,

a) 상기 가입자 단말과 현재 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 특정 시간이 경과한 때, 상기 현재의 트래픽 암호화 키를 갱신하기 위해 새로운 트래픽 암호화 키를 생성하는 단계; 및

b) 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 브로드캐스트 커넥션(Broadcast Connection)을 통해 상기 생성된 새로운 트래픽 암호화 키를 송신하여 상기 가입자 단말에서 사용되는 트래픽 암호화 키가 갱신되도록 하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 2】

무선 휴대 인터넷 시스템에서 기지국이 무선 연결된 가입자 단말에 대한 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하는 방

법에 있어서,

a) 상기 가입자 단말과 현재 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 특정 시간이 경과하기 전에 트래픽 암호화 키를 암호화하거나 복호하는데 사용되는 특정 키를 생성하는 단계;

b) 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 프라이머리 매니지먼트 커넥션(Primary Management Connection)을 통해 상기 생성된 특정 키를 각각 송신하는 단계;

c) 상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 상기 특정 시간이 경과한 때, 상기 현재의 트래픽 암호화 키를 갱신하기 위해 새로운 트래픽 암호화 키를 생성하는 단계; 및

d) 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 브로드캐스트 커넥션(Broadcast Connection)을 통해 상기 생성된 새로운 트래픽 암호화 키를 송신하여 상기 가입자 단말에서 사용되는 트래픽 암호화 키가 갱신되도록 하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 3】

제1항 또는 제2항에 있어서,

상기 특정 시간은 상기 기지국이 내부적으로 관리하는 멀티미디어 또는 브로

드캐스트 서비스용 트래픽 암호화 키 갱신 시간(M&B TEK Grace Time)에 기초하여 설정되며, 상기 현재의 트래픽 암호화 키의 유효 시간의 만료 시점으로부터 상기 M&B TEK Grace Time만큼 이전의 시간으로 설정되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 4】

제1항에 있어서,

상기 b) 단계에서, 상기 생성된 새로운 트래픽 암호화 키를 브로드캐스트 커넥션을 통해 상기 가입자 단말에게 송신할 때 IEEE 802.16에서의 보안 키 관리 프로토콜 메시지인 PKM-RSP(Privacy Key Management Response) 메시지의 한 메시지인 Key Reply 메시지를 이용하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 5】

제1항에 있어서,

상기 a) 단계에서, 상기 생성되는 새로운 트래픽 암호화 키는 3-DES(Data Encryption Standard) 방식 또는 AES(Advanced Encryption Standard) 방식을 통해 암호화되며, 상기 현재의 트래픽 암호화 키를 사용하여 암호화되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 6】

제1항에 있어서,

상기 a) 단계 전에,

i) 최초의 멀티캐스트 또는 브로드캐스트 서비스를 제공받기 위해 상기 가입자 단말로부터 멀티캐스트 또는 브로드캐스트 서비스용 트래픽 암호화 키를 요청받는 단계; 및

ii) 상기 요청된 멀티캐스트 또는 브로드캐스트 서비스용 트래픽 암호화 키를 생성하여 상기 가입자 단말로 송신하는 단계

를 더 포함하며,

상기 가입자 단말과의 메시지 송수신은 IEEE 802.16에서의 프라이머리 매니지먼트 커넥셔(Primary Management Connection)을 통해 이루어지는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 7】

제6항에 있어서,

상기 ii) 단계에서 생성되는 트래픽 암호화 키는 3-DES(Data Encryption Standard) 방식 또는 AES(Advanced Encryption Standard) 방식을 통해 암호화되며,

상기 가입자 단말의 인증키(Authentication Key)로부터 만들어진 KEK(Key Encryption Key)에 의해 암호화되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 8】

제1항에 있어서,

상기 b) 단계에서, 상기 생성된 새로운 트래픽 암호화 키가 상기 가입자 단말로 송신되어 갱신된 후 기존에 할당된 트래픽 암호화 키에 대한 유효 시간이 만료된 후부터 상기 새로운 트래픽 암호화 키의 유효 시간이 시작되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 9】

제2항에 있어서,

상기 b) 단계에서,

상기 특정 키는 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 동일하게 분배되어 있는 그룹 키 암호 키(Group Key Encryption Key:GKEK)인 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 10】

제9항에 있어서,

상기 GKEK는 상기 멀티캐스트 서비스 또는 브로드캐스트 서비스를 제공받고 있는 상기 가입자 단말에게 전달 시에 상기 가입자 단말의 인증키를 통해 암호화되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 11】

제2항에 있어서,

상기 a) 단계 전에,

i) 최초의 멀티캐스트 또는 브로드캐스트 서비스를 제공받기 위해 상기 가입자 단말로부터 멀티캐스트 또는 브로드캐스트 서비스용 트래픽 암호화 키를 요청받는 단계; 및

ii) 상기 요청된 멀티캐스트 또는 브로드캐스트 서비스용 트래픽 암호화 키를 생성하여 상기 가입자 단말로 송신하는 단계

를 더 포함하며,

상기 가입자 단말과의 메시지 송수신은 IEEE 802.16에서의 프라이머리 매니지먼트 커넥션을 통해 이루어지는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 12】

제11항에 있어서,

상기 ii) 단계에서 상기 생성된 트래픽 암호화 키를 상기 가입자 단말로 송신할 때 IEEE 802.16에서의 보안 키 관리 프로토콜 메시지인 PKM-RSP(Privacy Key Management Response) 메시지의 한 메시지인 Key Reply 메시지를 이용하며,

상기 Key Reply 메시지에는 상기 트래픽 암호화 키를 암호화하는데 사용된

상기 특정 키가 포함된

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 13】

제9항, 제10항 및 제12항 중 어느 한 항에 있어서,

상기 멀티캐스트 서비스별 또는 브로드캐스트 서비스별로 각각 관리되는 상기 GKEK는 상기 기지국 또는 상기 기지국에 접속되어 상기 가입자에 대한 인증을 수행하는 인증 서버(AAA:Authentication Authorization and Accounting 서버)에 의해 랜덤하게 생성되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 14】

제13항에 있어서,

상기 멀티캐스트 또는 브로드캐스트 서비스의 범위가 하나의 기지국에 국한되는 경우, 상기 기지국이 상기 GKEK를 랜덤하게 생성하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 15】

제13항에 있어서,

상기 멀티캐스트 또는 브로드캐스트 서비스의 범위가 상기 무선 휴대 인터넷 시스템의 전체인 경우, 상기 인증 서버가 상기 GKEK를 랜덤하게 생성하는 것을 특

징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 16】

제2항에 있어서,

상기 c) 단계에서,

상기 생성되는 새로운 트래픽 암호화 키는 3-DES(Data Encryption Standard) 방식 또는 AES(Advanced Encryption Standard) 방식을 통해 암호화되며, 상기 b) 단계에서 상기 가입자 단말로 송신된 특정 키에 의해 암호화된

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 17】

제2항에 있어서,

상기 d) 단계에서, 상기 생성된 새로운 트래픽 암호화 키가 상기 가입자 단말로 송신되어 갱신된 후, 상기 현재의 트래픽 암호화 키의 유효 시간이 만료되는 시점부터 상기 새로운 트래픽 암호화 키의 유효 시간이 시작되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 18】

제1항 또는 제2항에 있어서,

상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 상기 특정 시간이 경과한 후에 최초의 멀티캐스트 또는 브로드캐스트 서비스를 제공받기 위해

상기 가입자 단말로부터 멀티캐스트 또는 브로드캐스트 서비스용 트래픽 암호화 키를 요청받는 경우,

상기 현재의 트래픽 암호화 키 및 상기 현재의 암호화 키를 갱신하기 위해 생성된 상기 새로운 트래픽 암호화 키 모두를 상기 트래픽 암호화 키를 요청한 가입자 단말로 송신하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 19】

제1항 또는 제2항에 있어서,

상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 상기 특정 시간이 경과한 후에 상기 멀티캐스트 서비스나 브로드캐스트 서비스를 이미 제공받고 있는 상태에서 상기 현재의 트래픽 암호화 키의 갱신을 위해 상기 가입자 단말로부터 멀티캐스트 또는 브로드캐스트 서비스용 트래픽 암호화 키를 요청받는 경우,

상기 현재의 트래픽 암호화 키를 갱신하기 위해 생성된 상기 새로운 트래픽 암호화 키를 상기 요청한 가입자 단말로 송신하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 20】

제18항 또는 제19항에 있어서,

상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 상기 특정 시간이 경과한 후에 발생되는 상기 트래픽 암호화 키 요청 및 송신 동작은 프라이머리 매니지먼트 커넥션을 통해 상기 기지국과 상기 가입자 단말마다 개별적으로 이루어지는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 방법.

【청구항 21】

무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용하는 트래픽 암호화 키를 관리하는 방법에 있어서,

a) 상기 기지국으로부터 브로드캐스트 커넥션(Broadcast Connection)을 통해 새로운 트래픽 암호화 키를 수신하는 단계; 및

b) 상기 수신된 새로운 트래픽 암호화 키로 현재의 트래픽 암호화 키를 갱신하여 이후부터 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 상기 갱신된 새로운 트래픽 암호화 키를 사용하는 단계

를 포함하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 22】

무선 휴대 인터넷 시스템에서 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용하는 트래픽 암호화 키를 관리하는 방법에 있어서,

a) 상기 기지국으로부터 트래픽 암호화 키를 복호하는데 사용되는 새로운 특정 키-여기서 새로운 특정 키는 각 가입자 단말 인증 시 할당된 인증키로 암호화되어 있음-를 프라이머리 매니지먼트 커넥션(Primary Management Connection)을 통해 수신하는 단계;

b) 상기 수신된 새로운 특정 키로 현재의 특정 키를 갱신하는 단계;

c) 상기 기지국으로부터 브로드캐스트 커넥션(Broadcast Connection)을 통해 새로운 트래픽 암호화 키-여기서 새로운 트래픽 암호화 키는 상기 b) 단계에서 수신된 새로운 특정 키로 암호화되어 있음-를 수신하는 단계; 및

d) 상기 수신된 새로운 트래픽 암호화 키를 상기 b) 단계에서 수신된 새로운 특정 키로 복호하여 현재의 트래픽 암호화 키를 갱신하고, 이후부터 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 상기 갱신된 새로운 트래픽 암호화 키를 사용하는 단계

를 포함하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 23】

제21항에 있어서,

상기 새로운 트래픽 암호화 키는 상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 제1 특정 시간이 경과한 후에 상기 기지국으로부터 수신되는 것을 특징으로 하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 24】

제22항에 있어서,

상기 새로운 특정 키는 상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 제1 특정 시간이 경과하기 전에 상기 기지국으로부터 수신되고,

상기 새로운 트래픽 암호화 키는 상기 현재의 트래픽 암호화 키의 유효 시간의 시작 시점으로부터 상기 제1 특정 시간이 경과한 후에 상기 기지국으로부터 수신되는

것을 특징으로 하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 25】

제23항 또는 제24항에 있어서,

상기 제1 특정 시간은 상기 기지국이 내부적으로 관리하는 멀티미디어 또는 브로드캐스트 서비스용 트래픽 암호화 키 갱신 시간(M&B TEK Grace Time)에 기초하

여 설정되며, 상기 현재의 트래픽 암호화 키의 유효 시간의 만료 시점으로부터 상기 M&B TEK Grace Time만큼 이전의 시간으로 설정되는 것을 특징으로 하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 26】

제25항에 있어서,

상기 가입자 단말은 제2 특정 시간이 경과하기 전에 상기 기지국으로부터 브로드캐스트 커넥션을 통해 새로운 트래픽 암호화 키가 수신되는 경우, 상기 가입자 단말 자체에 의한 트래픽 암호화 키 갱신 요청을 수행하지 않는 것을 특징으로 하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 27】

제26항에 있어서,

상기 제2 특정 시간은 상기 가입자 단말이 내부적으로 관리하는 트래픽 암호화 키 갱신 시간(TEK Grace Time)에 기초하여 설정되며, 상기 현재의 트래픽 암호화 키의 유효 시간의 만료 시점으로부터 상기 TEK Grace Time만큼 이전의 시간으로 설정되는 것을 특징으로 하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 28】

제27항에 있어서,

상기 M&B TEK Grace Time이 상기 TEK Grace Time보다 크도록 설정되는 것을

특징으로 하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 29】

제23항 또는 제24항에 있어서,

상기 현재의 트래픽 암호화 키가 상기 새로운 트래픽 암호화 키로 갱신된 후, 상기 현재의 트래픽 암호화 키의 유효 시간이 만료되는 시점부터 상기 새로운 트래픽 암호화 키의 유효 시간이 시작되는 것을 특징으로 하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 30】

제25항에 있어서,

상기 제2 특정 시간이 경과할 때까지 상기 기지국으로부터 브로드캐스트 커넥션을 통해 새로운 트래픽 암호화 키가 수신되지 않은 경우,

상기 현재의 트래픽 암호화 키를 갱신하기 위해 프라이머리 매니지먼트 커넥션을 통해 새로운 트래픽 암호화 키를 상기 기지국으로 요청하여 수신하는 단계;

상기 수신된 새로운 트래픽 암호화 키로 현재의 트래픽 암호화 키를 갱신하여 이후부터 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 상기 갱신된 새로운 트래픽 암호화 키를 사용하는 단계

를 포함하는 무선 휴대 인터넷 시스템의 가입자 단말에서의 트래픽 암호화 키 관리 방법.

【청구항 31】

무선 휴대 인터넷 시스템에서 가입자 단말과 기지국 간에 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키에 대한 관리를 수행하기 위한 프로토콜을 구성하는 방법에 있어서,

a) 상기 가입자 단말이 트래픽 암호화 키를 요청하는 키 요청(Key Request) 메시지를 MAC 메시지를 이용하여 상기 기지국으로 송신하는 단계;

b) 상기 기지국이 상기 요청된 트래픽 암호화 키와 특정 키-여기서 특정 키는 상기 가입자 단말에게 할당된 인증키로 암호화되어 있고, 상기 트래픽 암호화 키를 암호화하는데 사용됨-를 포함하는 키 응답(Key Reply) 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계;

c) 상기 특정 키를 갱신하기 위해 상기 기지국이 새로운 특정 키를 포함하는 제1 키 갱신 명령(Key Update Command) 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계; 및

d) 상기 트래픽 암호화 키를 갱신하기 위해 상기 기지국이 새로운 트래픽 암호화 키-여기서 새로운 트래픽 암호화 키는 상기 새로운 특정 키에 의해 암호화됨-를 포함하는 제2 키 갱신 명령 메시지를 MAC 메시지를 이용하여 상기 가입자 단말로 송신하는 단계

를 포함하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토

콜 구성 방법.

【청구항 32】

제31항에 있어서,

상기 a) 단계에서,

상기 키 요청 메시지는 IEEE 802.16에서의 보안 키 관리 프로토콜 메시지인 PKM-REQ(Privacy Key Management Request) 메시지의 한 메시지인 Key Request 메시지를 통해 프라이머리 매니지먼트 커넥션(Primary Management Connection)으로 송신되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법.

【청구항 33】

제31항에 있어서,

상기 b) 단계에서,

상기 키 응답 메시지는 IEEE 802.16에서의 보안 키 관리 프로토콜 메시지인 PKM-RSP(Privacy Key Management Response) 메시지의 한 메시지인 Key Reply 메시지를 통해 프라이머리 매니지먼트 커넥션(Primary Management Connection)으로 송신되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법.

【청구항 34】

제33항에 있어서,

상기 특정 키는 상기 멀티캐스트 또는 브로드캐스트 서비스를 제공받고 있는 가입자 단말 모두에게 동일하게 분배되어 있는 그룹 키 암호화 키(Group Key Encryption Key:GKEK)이며, 상기 Key Reply 메시지의 파라미터 중 하나인 트래픽 암호화 키 파라미터(TEK-Parameters)에 포함되어 전송되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법.

【청구항 35】

제31항에 있어서,

상기 c) 단계 및 d) 단계에서,

상기 제1 키 갱신 명령 메시지는 프라이머리 매니지먼트 커넥션을 통해 전송되고,

상기 제2 키 갱신 명령 메시지는 브로드캐스트 커넥션을 통해 전송되며,

상기 제1 키 갱신 명령 메시지 및 제2 키 갱신 명령 메시지에는,

가입자 단말 인증키 일련 번호(Key-Sequence-Number) 파라미터, SA(Security Association)의 식별자(Identication)인 SAID 파라미터, 상기 제1 키 갱신 명령 메시지와 상기 제2 키 갱신 명령 메시지를 구분하기 위한 키 푸시 모드(Key Push Mode) 파라미터, 키 갱신 명령 메시지에 대한 리플레이 공격(Replay Attack)을 방지하기 위한 키 푸시 카운터(Key Push Counter), 트래픽 암호화 키와 관련된 정보인 파라미터(TEK-Parameters) 및 상기 제1 키 갱신 명령 메시지와 상기 제2 키 갱신 명령 메시지 자체를 인증하기 위한 파라미터(HMAC-Digest)가 포함되는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법.

【청구항 36】

제35항에 있어서,

상기 제1 키 갱신 명령 메시지에 포함된 TEK-Parameters에는 상기 GKEK 및 트래픽 암호화 키 일련 번호가 포함되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법.

【청구항 37】

제35항에 있어서,

상기 제2 키 갱신 명령 메시지에 포함된 TEK-Parameters에는 상기 새로운 트래픽 암호화 키, 상기 새로운 트래픽 암호화 키의 유효 시간, 상기 새로운 트래픽 암호화 키 일련 번호 및 트래픽 데이터를 암호화하는데 필요한 입력 키 역할을 하는 CBC(Cipher Block Chaining)-IV(Initialization Vector)가 포함되는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법.

【청구항 38】

제35항에 있어서,

상기 키 갱신 명령 메시지에 포함된 HMAC-Digest를 생성하는데 입력키로써 필요한 HMAC 인증 키(HMAC authentication key)를 하향링크에 대하여 생성하는 경

우,

SHA(Secure Hash Algorithm) 방식을 사용하여 상기 HMAC 인증 키를 생성하고, 이 때의 입력키로,

상기 제1 키 갱신 명령 메시지 및 제2 키 갱신 명령 메시지에는 하향 링크 HMAC_PAD_D와 리플레이 공격(Replay Attack)을 방지하기 위한 키 푸시 카운터(Key Push Counter)가 공히 사용되며,

상기 제1 키 갱신 명령 메시지에는 가입자 단말별로 할당한 인증키가 또 다른 입력키로 사용되고, 상기 제2 키 갱신 명령 메시지에는 상기 제1 키 갱신 명령 메시지를 통해 전달한 GKEK가 또 다른 입력키로 사용되는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 관리 프로토콜 구성 방법.

【청구항 39】

무선 휴대 인터넷 시스템에서 가입자 단말에 구비되며, 상기 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하기 위한 트래픽 암호화 키 상태 머신의 동작 방법에 있어서,

상기 기지국으로 트래픽 암호화 키를 요청하는 키 요청 메시지 송신 이벤트(event)에 의해 키 요청(Key Request) 메시지를 송신하고 대기하는 동작 대기 단계

(Op Wait); 및

상기 기지국과의 정상적인 트래픽 데이터의 송수신 동작을 수행하는 동작 단계(Operational)

를 포함하며,

상기 트래픽 암호화 키 상태 머신은,

상기 동작 대기 단계에서 상기 기지국으로부터 트래픽 암호화 키를 수신하는 키 응답 메시지 수신 이벤트 발생에 의해 상기 동작 단계로 천이되어 동작하고,

상기 동작 단계에서 상기 새로운 트래픽 암호화 키가 포함된 키 응답 메시지를 수신하였을 경우, 동작 단계에서 머무르게 되는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 상태 머신의 동작 방법.

【청구항 40】

제39항에 있어서,

상기 가입자 단말의 요청에 의해 상기 기지국에서 생성되어 송신되는 새로운 트래픽 암호화 키를 사용하여 갱신하기 위해 대기하는 갱신 대기 단계(Rekey Wait)를 더 포함하며,

상기 동작 단계에서 상기 기지국으로부터 상기 새로운 트래픽 암호화 키를 분배하기 위해 사용되는 키 응답 메시지를 수신하지 못하였을 경우, 상기 단말의 트래픽 암호화 키 갱신 이벤트(TEK Refresh Timeout) 발생에 의해 상기 단말이 상

기 기지국으로 키 요청(Key Request) 메시지를 송신하고, 상기 트래픽 암호화 키 상태 머신이 상기 갱신 대기 단계로 천이하여 동작하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 상태 머신의 동작 방법.

【청구항 41】

제40항에 있어서,

상기 갱신 대기 단계에서 상기 단말로부터 키 요청 메시지에 대한 상기 기지국의 응답으로 새로운 트래픽 암호화 키가 포함된 키 응답(Key Reply) 메시지를 수신하여 상기 트래픽 암호화 키 상태 머신이 상기 동작 단계로 천이되어 동작하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 상태 머신의 동작 방법.

【청구항 42】

무선 휴대 인터넷 시스템에서 가입자 단말에 구비되며, 상기 기지국에 무선 연결된 가입자 단말이 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) 서비스를 위해 상기 기지국과 송수신하는 트래픽 데이터를 암호화 또는 복호하는데 사용되는 트래픽 암호화 키를 관리하기 위한 트래픽 암호화 키 상태 머신의 동작 방법에 있어서,

상기 기지국으로 트래픽 암호화 키를 요청하는 키 요청 메시지 송신 이벤트(event)에 의해 키 요청(Key Request) 메시지를 송신하고 대기하는 동작 대기 단계

(Op Wait);

상기 기지국과의 정상적인 트래픽 데이터의 송수신 동작을 수행하는 동작 단계(Operational); 및

상기 기지국에서 자동으로 생성되어 송신되는 새로운 트래픽 암호화 키를 사용하여 갱신하기 위해 대기하는 M&B(Multicast & Broadcast) 갱신 잠정 대기 단계(M&B Rekey Interim Wait)

를 포함하며,

상기 트래픽 암호화 키 상태 머신은,

상기 동작 대기 단계에서 상기 기지국으로부터 트래픽 암호화 키를 수신하는 키 응답 메시지 수신 이벤트 발생에 의해 상기 동작 단계로 천이되어 동작하고,

상기 동작 단계에서 상기 특정 키를 갱신하기 위해 상기 기지국으로부터 제1 키 갱신 명령 메시지를 통해 새로운 특정 키를 수신하였을 경우, GKEK Updated 이벤트가 발생하게 되고, 이로 인해 상기 M&B 갱신 잠정 대기 단계로 천이하여 동작하며,

상기 M&B 갱신 잠정 대기 단계에서 상기 새로운 특정 키로 암호화된 새로운 트래픽 암호화 키를 상기 기지국으로부터 브로드캐스트 커넥션을 통해 제2 키 갱신 명령 메시지를 수신하였을 경우, TEK Updated 이벤트가 발생하게 되고, 이로 인해 상기 동작 단계로 천이되어 동작하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 상태

머신의 동작 방법.

【청구항 43】

제42항에 있어서,

상기 가입자 단말의 요청에 의해 상기 기지국에서 생성되어 송신되는 새로운 트래픽 암호화 키를 사용하여 갱신하기 위해 대기하는 갱신 대기 단계(Rekey Wait)를 더 포함하며,

상기 동작 단계에서 상기 기지국으로부터 상기 새로운 특정 키를 분배하기 위해 사용되는 상기 제1 키 갱신 명령 메시지를 수신하지 못하여 GKEK Updated 이벤트가 발생하지 않은 경우, 상기 단말의 트래픽 암호화 키 갱신 이벤트(TEK Refresh Timeout) 발생에 의해 상기 단말은 상기 기지국으로 키 요청(Key Request) 메시지를 송신하고, 상기 트래픽 암호화 키 상태 머신이 상기 갱신 대기 단계로 천이하여 동작하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 상태 머신의 동작 방법.

【청구항 44】

제43항에 있어서,

상기 M&B 갱신 잠정 대기 단계에서 상기 기지국으로부터 상기 새로운 트래픽 암호화 키를 분배하기 위해 사용되는 상기 제2 키 갱신 명령 메시지를 수신하지 못하여 TEK Updated 이벤트가 발생하지 않은 경우, 상기 단말의 트래픽 암호화 키 갱

신 이벤트(TEK Refresh Timeout) 발생에 의해 상기 단말은 상기 기지국으로 키 요청(Key Request) 메시지를 송신하고, 상기 트래픽 암호화 키 상태 머신이 상기 갱신 대기 단계로 천이하여 동작하는

것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 상태 머신의 동작 방법.

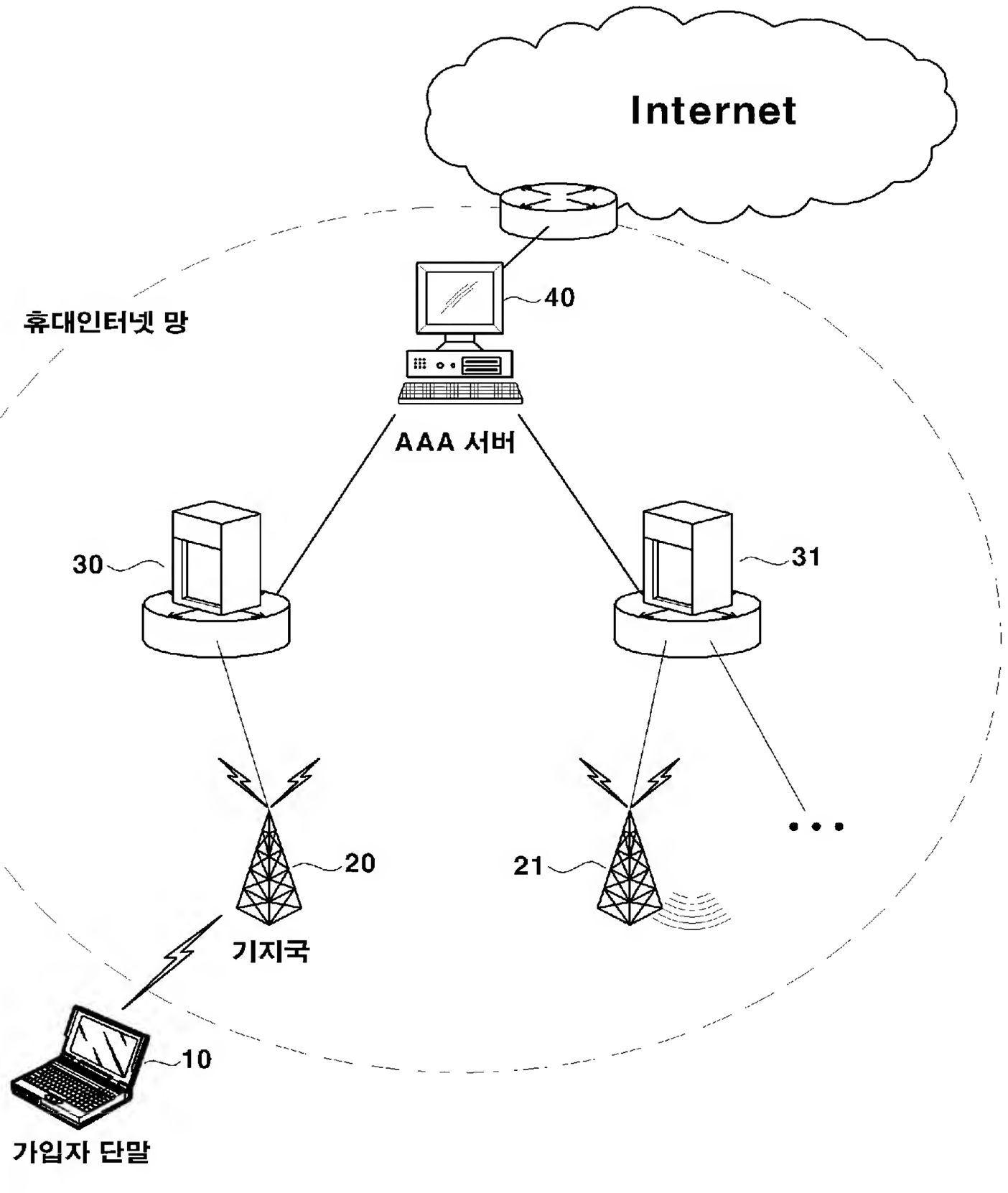
【청구항 45】

제43항 또는 제 44항에 있어서,

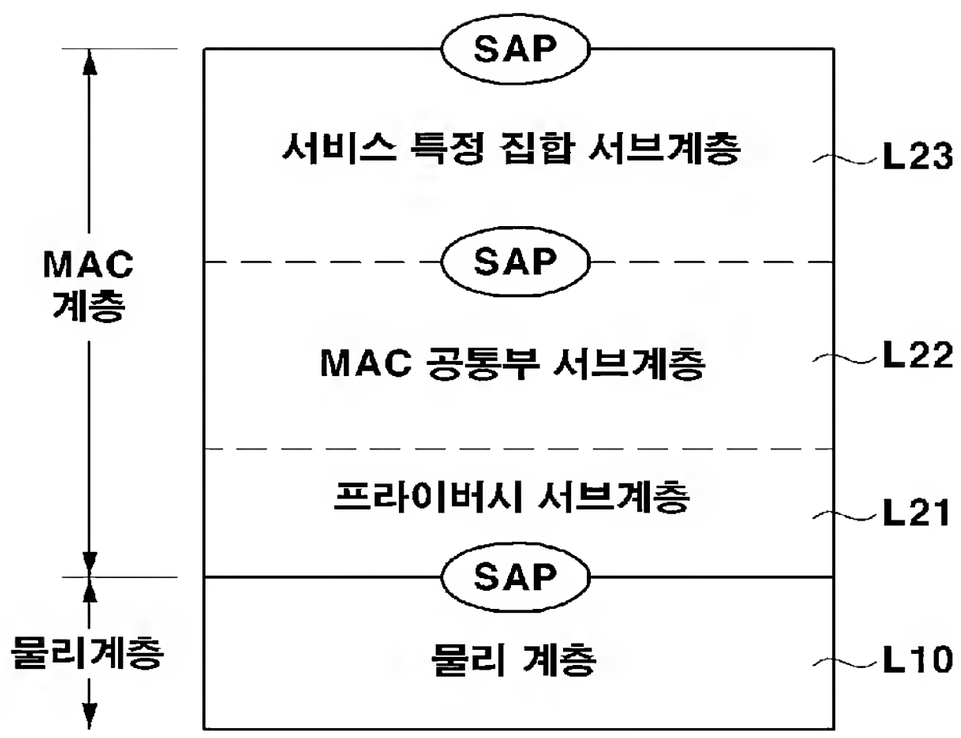
상기 갱신 대기 단계에서 상기 단말로부터 키 요청 메시지에 대한 상기 기지국의 응답으로 새로운 트래픽 암호화 키 및 상기 새로운 트래픽 암호화 키를 복호하는데 사용되는 새로운 특정 키가 포함된 키 응답(Key Reply) 메시지를 수신하여 상기 트래픽 암호화 키 상태 머신이 상기 동작 단계로 천이되어 동작하는 것을 특징으로 하는 무선 휴대 인터넷 시스템에서의 트래픽 암호화 키 상태 머신의 동작 방법.

【도면】

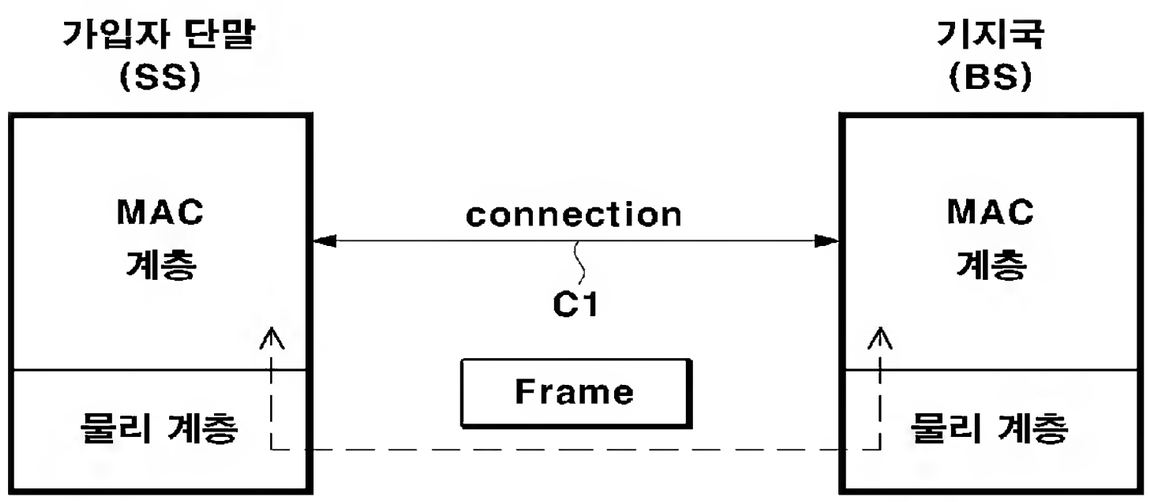
【도 1】



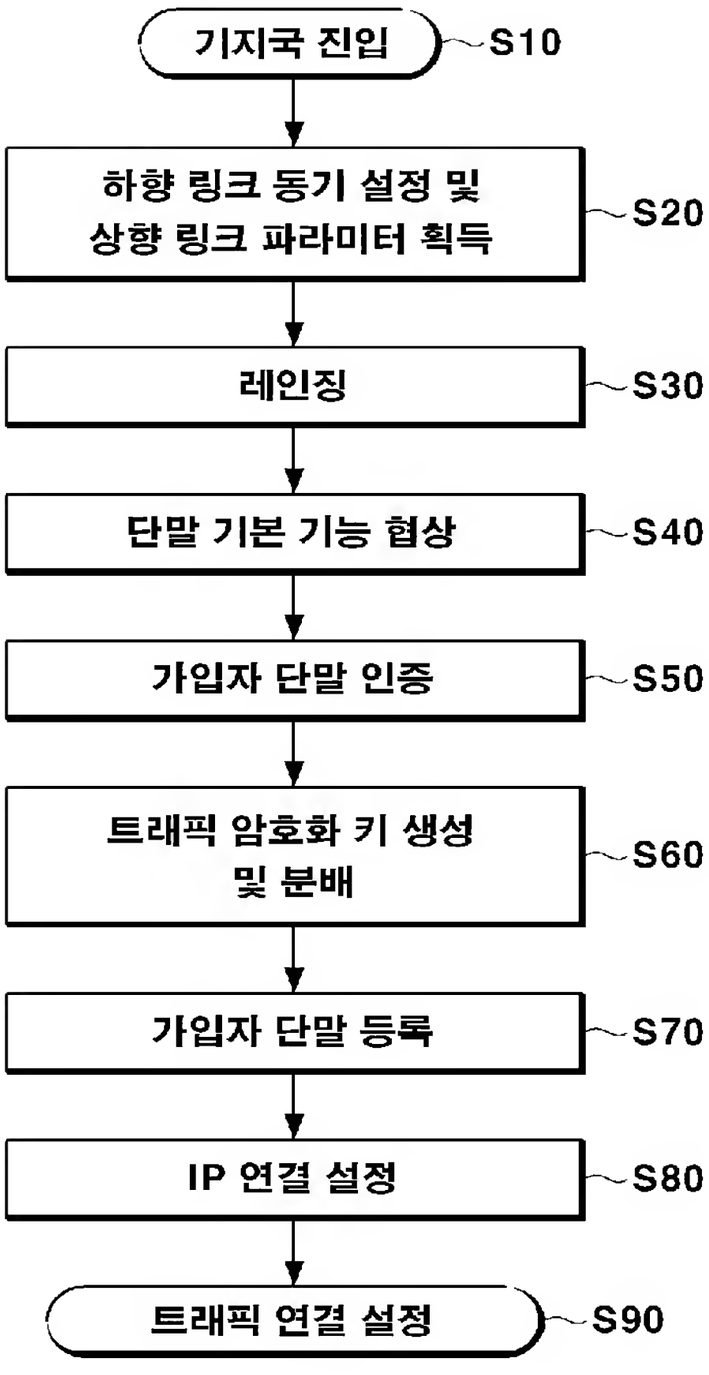
【도 2】


SAP
서비스 특정 집합 서브계층
L23
SAP
MAC 공통부 서브계층
L22
프라이버시 서브계층
L21
SAP
물리 계층
L10
MAC 계층
물리계층

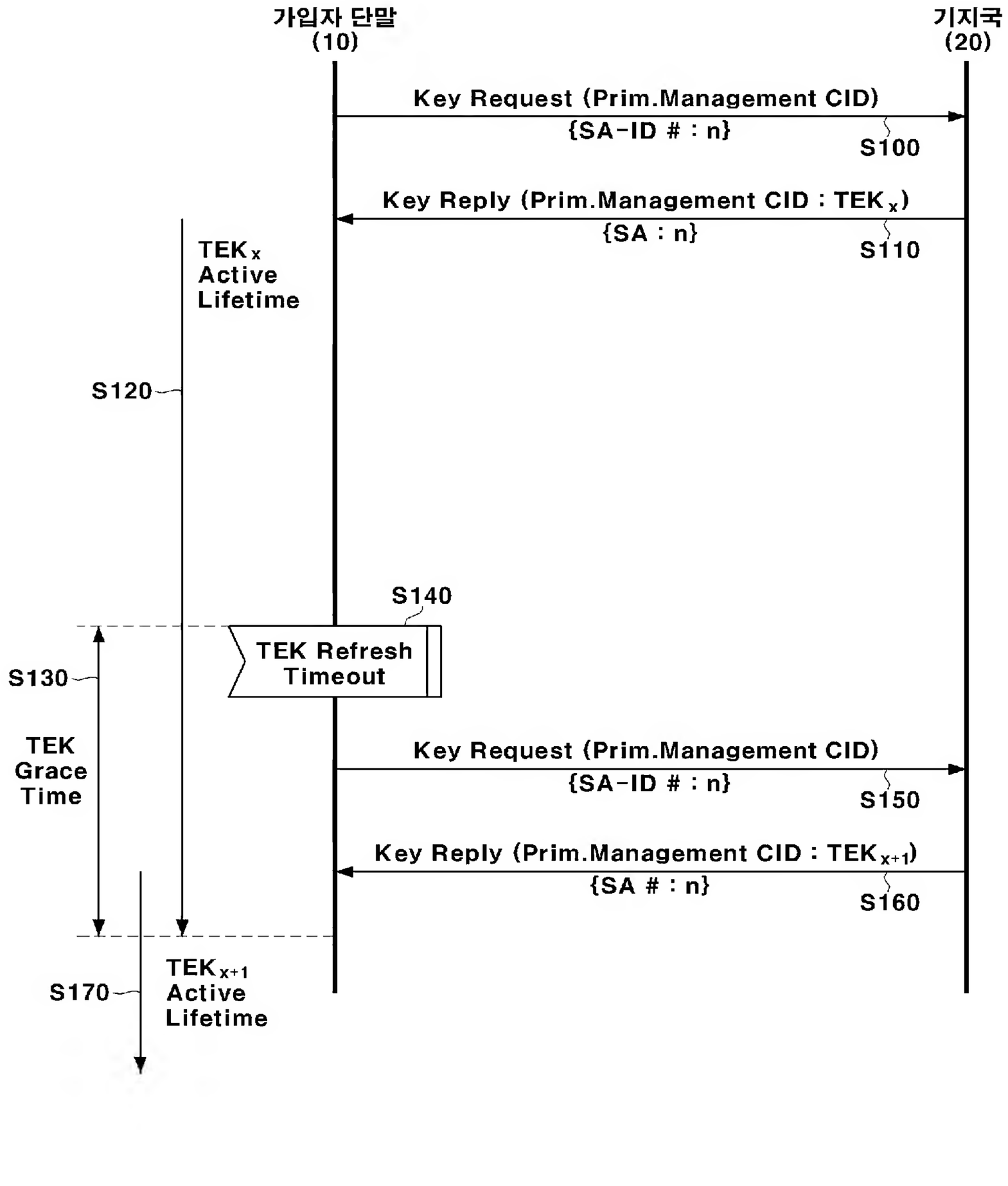
【도 3】


가입자 단말 (SS)
기지국 (BS)
MAC 계층
connection
C1
MAC 계층
Frame
물리 계층
물리 계층

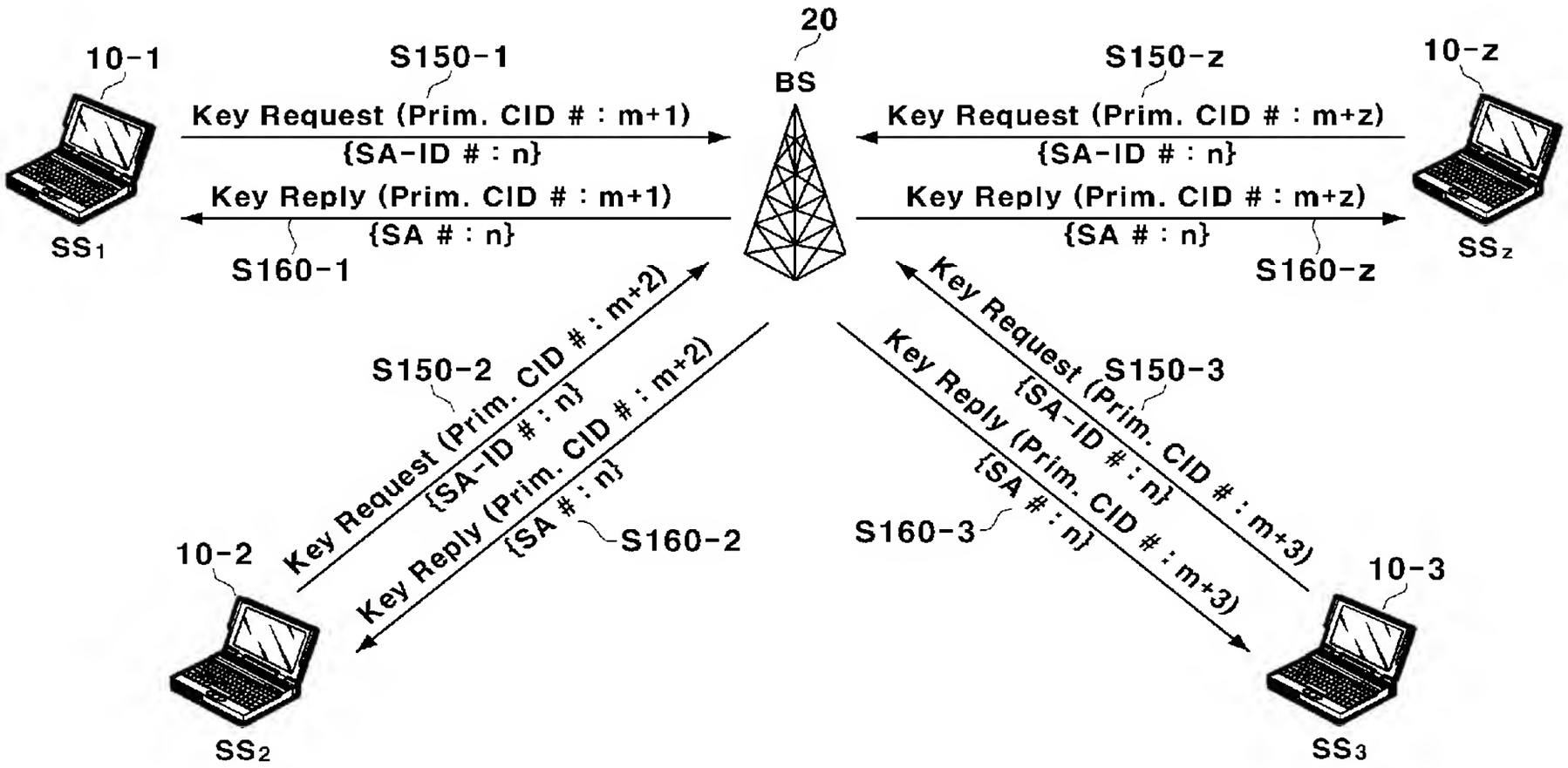
【도 4】


기지국 진입
S10
하향 링크 동기 설정 및
상향 링크 파라미터 획득
S20
레인징
S30
단말 기본 기능 협상
S40
가입자 단말 인증
S50
트래픽 암호화 키 생성
및 분배
S60
가입자 단말 등록
S70
IP 연결 설정
S80
트래픽 연결 설정
S90

【도 5】


가입자 단말
(10)
기지국
(20)
Key Request (Prim.Management CID)
{SA-ID # : n}
S100
Key Reply (Prim.Management CID : TEK x)
{SA : n}
S110
TEK x
Active
Lifetime
S120
S140
TEK Refresh
Timeout
S130
TEK
Grace
Time
Key Request (Prim.Management CID)
{SA-ID # : n}
S150
Key Reply (Prim.Management CID : TEK x+1)
{SA # : n}
S160
S170
TEK x+1
Active
Lifetime

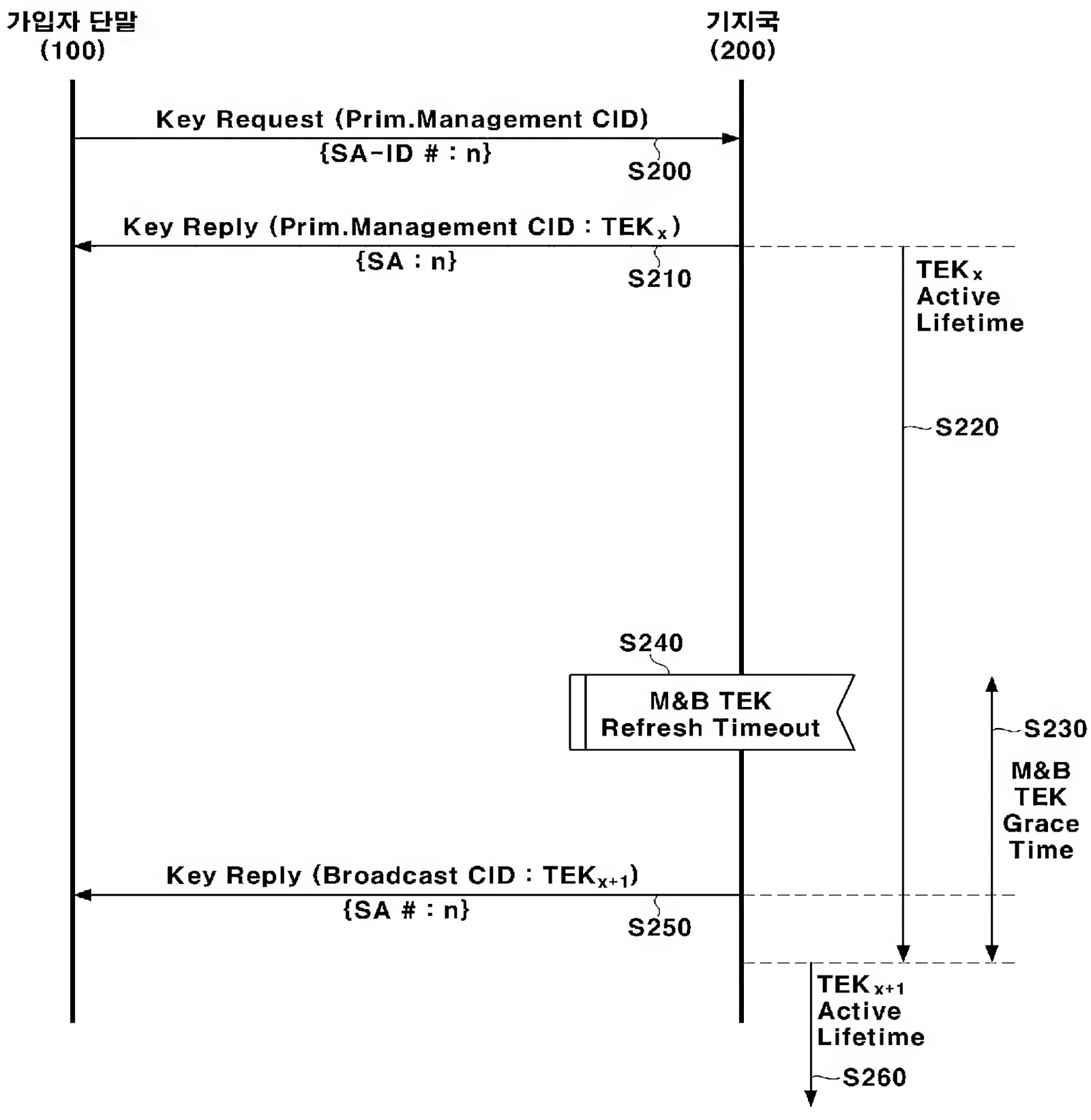
【도 6】



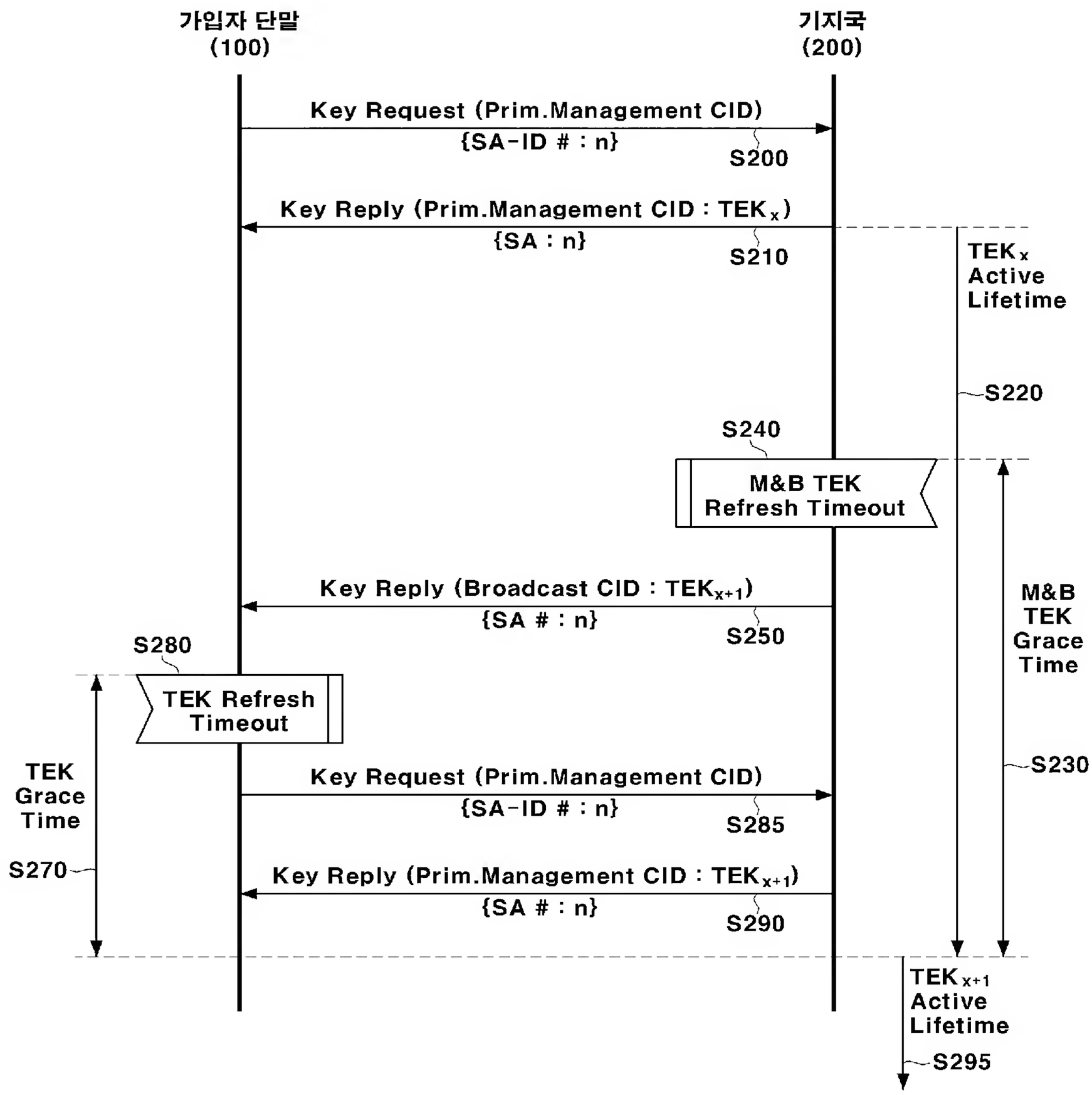
【도 7】

System	Name	Description	Minimum value	Default value	Maximum value
BS	M&B TEK Grace Time	Time prior to TEK (for the multicast and broadcast traffic service) expiration BS begins rekeying. This time is longer than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value

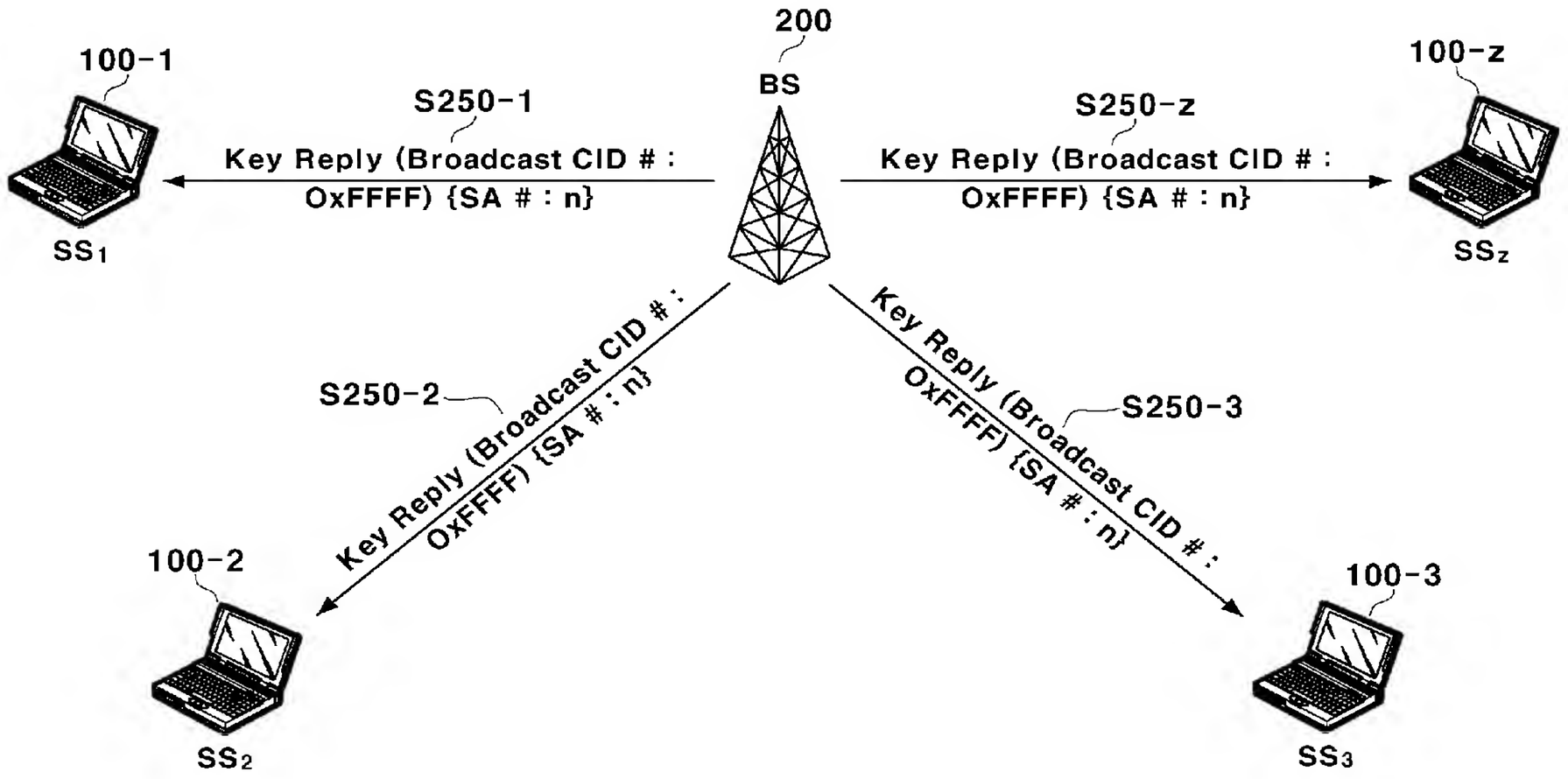
【도 8】


가입자 단말
(100)
기지국
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S200
Key Reply (Prim.Management CID : TEKx)
{SA : n}
S210
TEKx
Active
Lifetime
S220
S240
M&B TEK
Refresh Timeout
S230
M&B
TEK
Grace
Time
Key Reply (Broadcast CID : TEKx+1)
{SA # : n}
S250
TEKx+1
Active
Lifetime
S260

【도 9】


가입자 단말
(100)
기지국
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S200
Key Reply (Prim.Management CID : TEKx)
{SA : n}
S210
TEKx
Active
Lifetime
S220
S240
M&B TEK
Refresh Timeout
Key Reply (Broadcast CID : TEKx+1)
{SA # : n}
S250
M&B
TEK
Grace
Time
S280
TEK Refresh
Timeout
TEK
Grace
Time
S230
Key Request (Prim.Management CID)
{SA-ID # : n}
S285
S270
Key Reply (Prim.Management CID : TEKx+1)
{SA # : n}
S290
TEKx+1
Active
Lifetime
S295

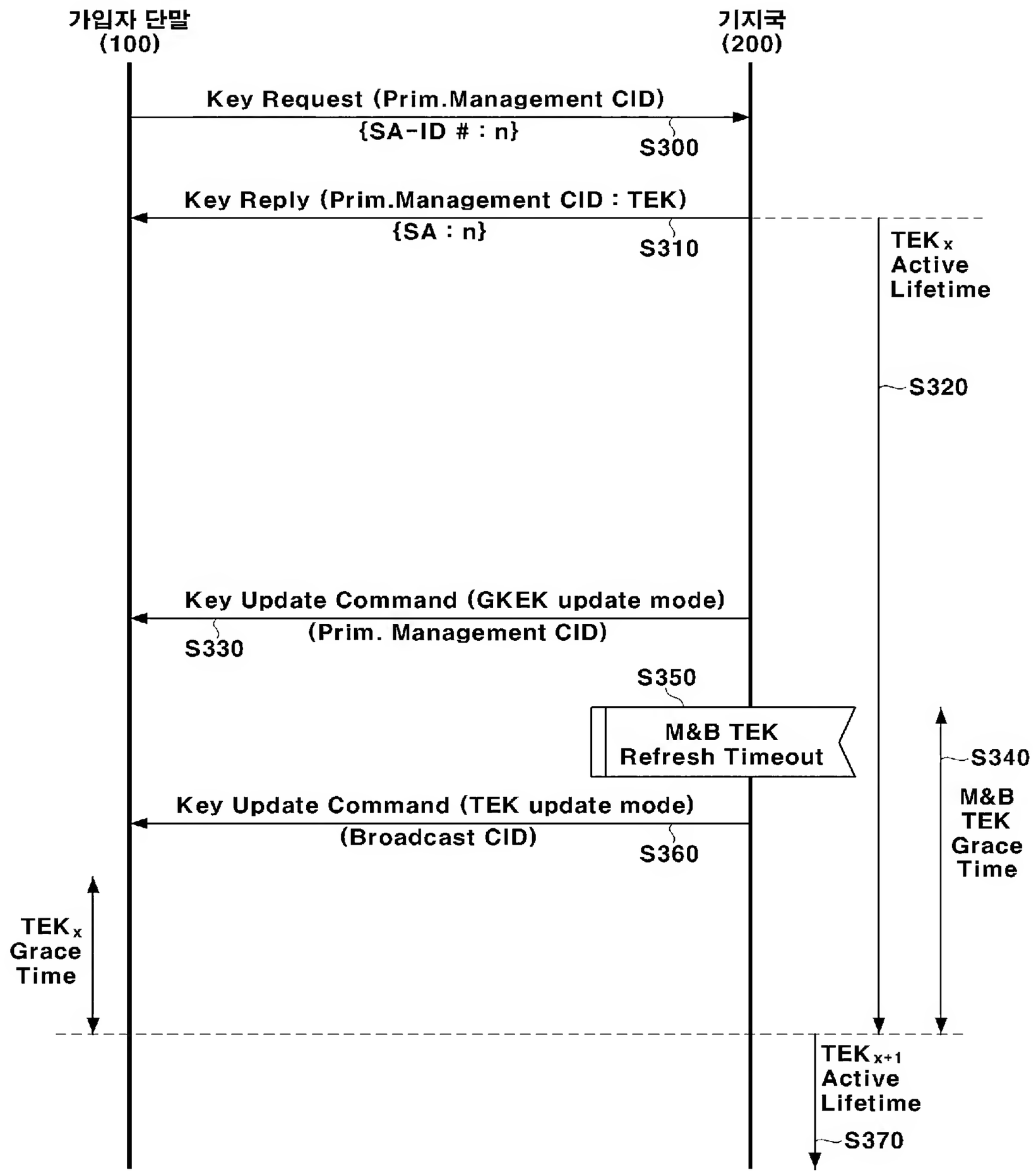
【도 10】



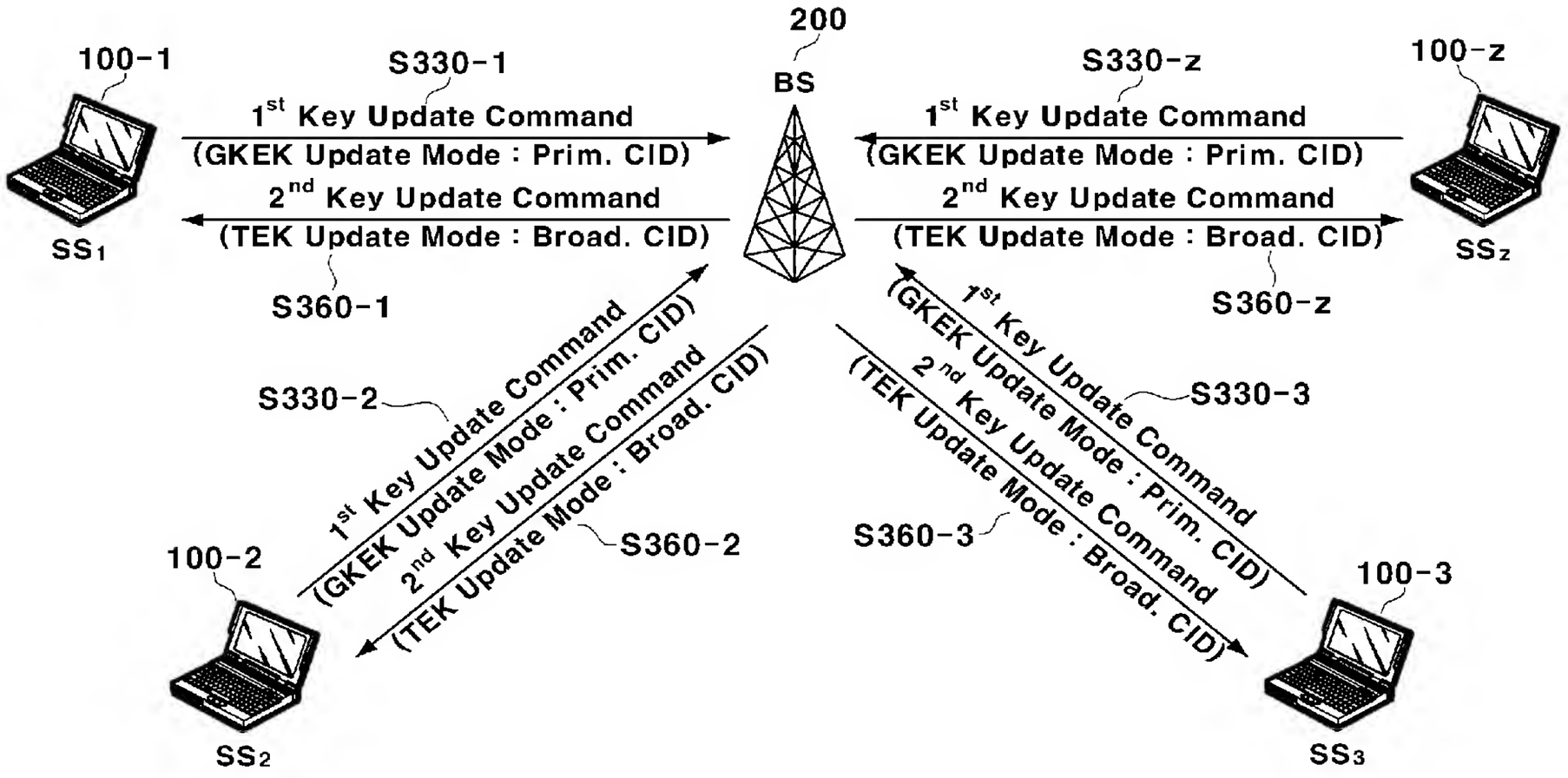
【도 11】

CID(MAC Header)	Key to encrypt the TEK
Primary Management CID	KEK(Derived from the AK)
Broadcast CID	Old distributed TEK

【도 12】


가입자 단말
(100)
기지국
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S300
Key Reply (Prim.Management CID : TEK)
{SA : n}
S310
TEKx
Active
Lifetime
S320
Key Update Command (GKEK update mode)
(Prim. Management CID)
S330
S350
M&B TEK
Refresh Timeout
S340
M&B
TEK
Grace
Time
Key Update Command (TEK update mode)
(Broadcast CID)
S360
TEKx
Grace
Time
TEKx+1
Active
Lifetime
S370

【도 13】



【도 14】

Attributes	Contents
Key-Sequece-Number	Authorization Key sequence number
SAID	Security Association ID
TEK-Parameters	"Older" generation of key parameters relevant to SAID
TEK-Parameters	"Newer" generation of key parameters relevant to SAID
HMAC-Digest	Keyed SHA message digest

【도 15】

Attribute	Contents
GKEK	GKEK, encrypted with the AK
TEK	TEK, encrypted with the GKEK (Multicast or Broadcast Service) or encrypted with the KEK (Unicast Service)
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequnce Number
CBC-IV	Cipher Block Chaining (CBC) Initialization Vector

【도 16】

Attributes	Contents	1st Message (Primary)	2nd Message (Braodcast)
Key-Sequence-Number	Authorization key sequence number	○	○
SAID	Security Association ID	○	○
Key Push Modes	Usage code of Key Update Command message	○	○
Key Push Counter	Counter one greater than that of older generation for reply attack	○	○
TEK-Parameters	"Newer" generation of key parameters relevant to SAID		
> GKEK	GKEK, encrypted with the AK	○	×
> TEK	TEK, encrypted with the GKEK(Multicast or Broadcast Service)	×	○
> Key-Lifetime	TEK Remaining Lifetime	×	○
> Key-Sequence-Number	TEK Sequnce Number	○	○
> CBS-IV	Cipher Block Chaining (CBC) Initialization Vector	×	○
HMAC-Digest	Keyed SHA message digest	○	○

【도 17】

Type	Length	Value
30	1	0, GKEK update mode (1st Message) 1, TEK update mode (2nd Message) 2-225, reserved

【도 18】

Key push modes	Input Key
GKEK update mode	AK
TEK update mode	GKEK

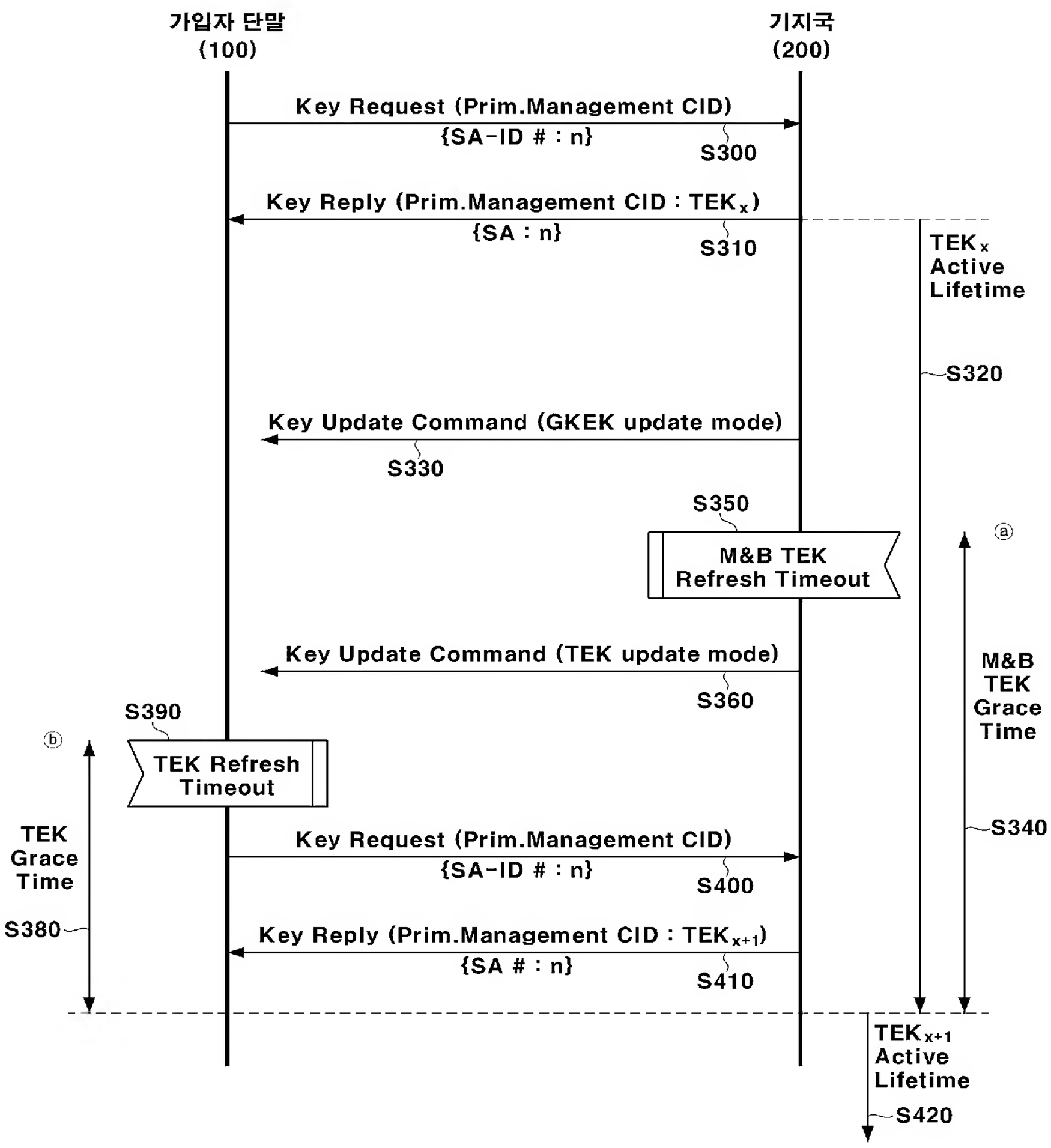
【도 20】

Situation	Transferred TEK-parameter information
Initial TEK response (before ⓐ)	$TEK\text{-}Parameters_C$
Initial TEK response (after ⓐ)	$TEK\text{-}Parameters_C$ & $TEK\text{-}Parameters_N$
TEK update response (after ⓑ)	$TEK\text{-}Parameters_N$

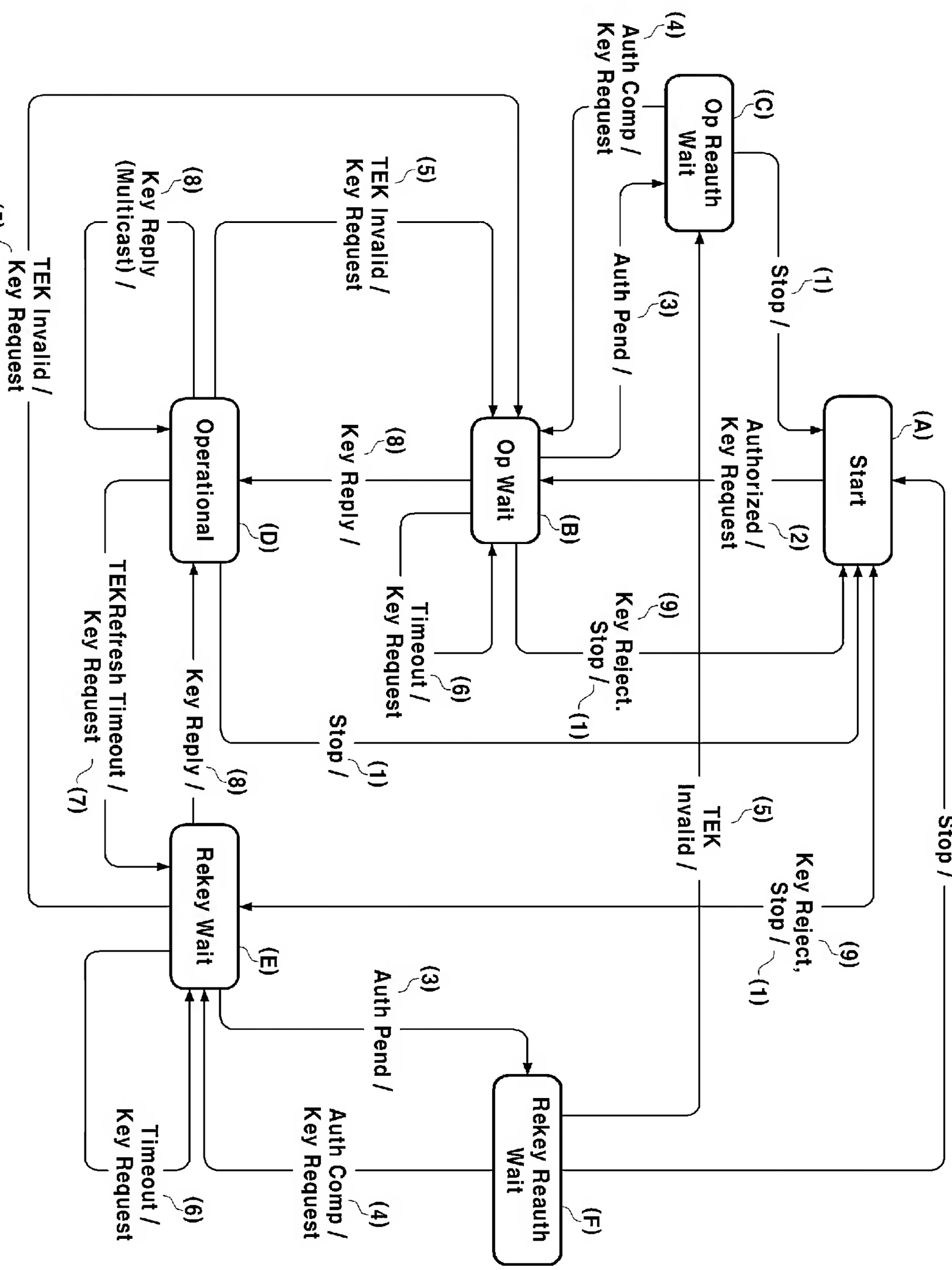
C: Current generation of key parameters relevant to SAID

N: Next generation of key parameters relevant to SAID

【도 19】

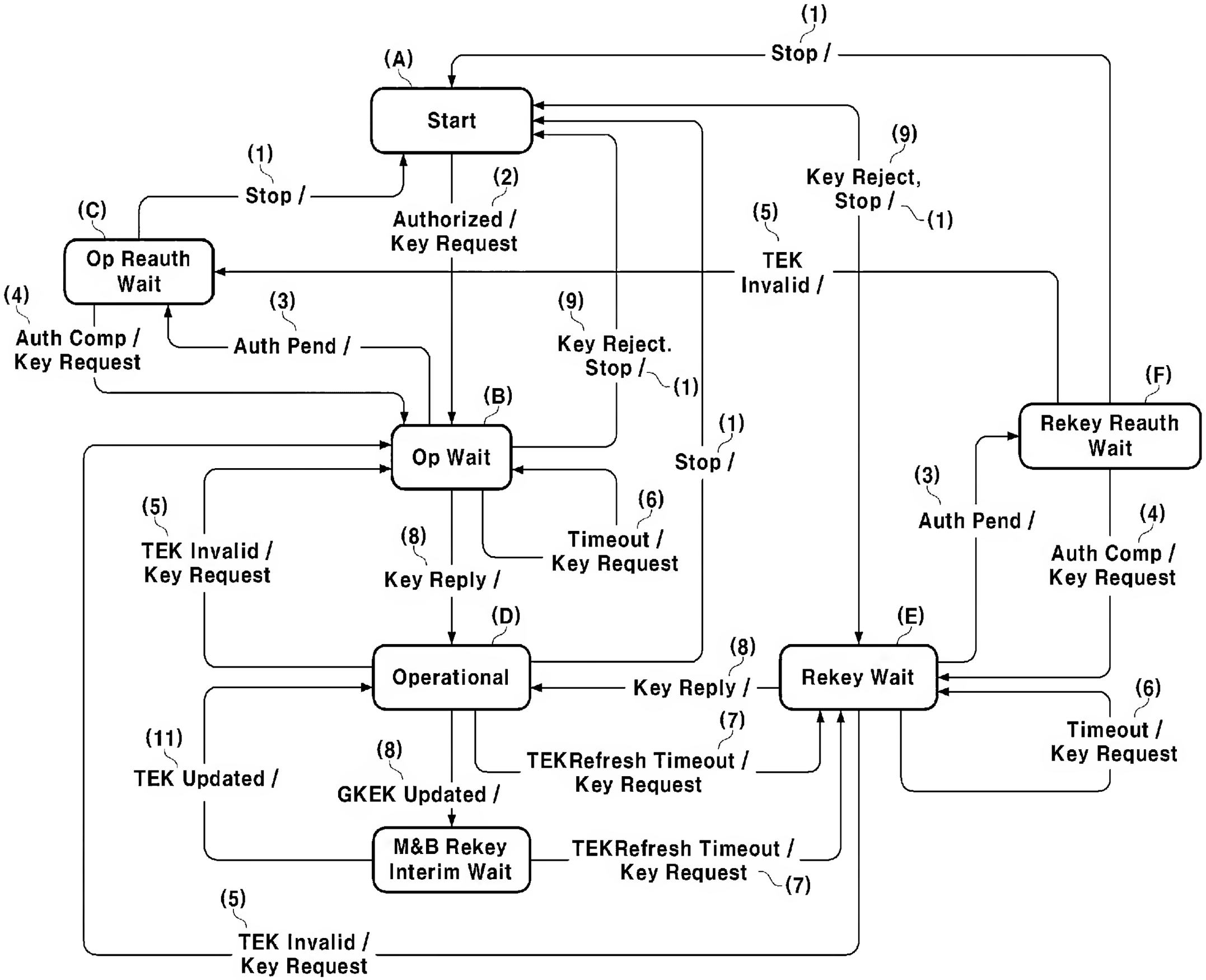

가입자 단말
(100)
기지국
(200)
Key Request (Prim.Management CID)
{SA-ID # : n}
S300
Key Reply (Prim.Management CID : TEKx)
{SA : n}
S310
TEKx
Active
Lifetime
S320
Key Update Command (GKEK update mode)
S330
S350
M&B TEK
Refresh Timeout
ⓐ
Key Update Command (TEK update mode)
S360
M&B
TEK
Grace
Time
S340
S390
ⓑ
TEK Refresh
Timeout
TEK
Grace
Time
S380
Key Request (Prim.Management CID)
{SA-ID # : n}
S400
Key Reply (Prim.Management CID : TEKx+1)
{SA # : n}
S410
TEKx+1
Active
Lifetime
S420

【도 21】


Start
(A)
Op Reauth Wait
(C)
Op Wait
(B)
Operational
(D)
Rekey Wait
(E)
Rekey Reauth Wait
(F)
(1) Stop /
(2) Authorized / Key Request
(3) Auth Pend /
(4) Auth Comp / Key Request
(5) TEK Invalid / Key Request
(6) Timeout / Key Request
(7) TEKRefresh Timeout / Key Request
(8) Key Reply / (Multicast) /
(9) Key Reject, Stop /

【도 22】

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(1) Stop		Start	Start	Start	Start	Start
(2) Authorized	Op Wait					
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait	
(4) Auth Comp			Op Wait			Rekey Wait
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait
(6) Timeout		Op Wait			Rekey Wait	
(7) TEK Refresh Timeout				Rekey Wait		
(8) Key Reply		Operational		Operational	Operational	
(9) Key Reject		Start			Start	


(A)
Start
(1)
Stop /
(1)
Stop /
(2)
Authorized /
Key Request
(9)
Key Reject,
Stop /
(1)
(C)
Op Reauth
Wait
(5)
TEK
Invalid /
(4)
Auth Comp /
Key Request
(3)
Auth Pend /
(9)
Key Reject.
Stop /
(1)
(B)
Op Wait
(1)
Stop /
(F)
Rekey Reauth
Wait
(5)
TEK Invalid /
Key Request
(8)
Key Reply /
(6)
Timeout /
Key Request
(3)
Auth Pend /
(4)
Auth Comp /
Key Request
(D)
(E)
Operational
(8)
Key Reply /
Rekey Wait
(6)
Timeout /
Key Request
(11)
TEK Updated /
(8)
GKEK Updated /
(7)
TEKRefresh Timeout /
Key Request
M&B Rekey
Interim Wait
TEKRefresh Timeout /
Key Request
(7)
(5)
TEK Invalid /
Key Request

【도 23】

100-99

【도 24】

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait	(G) M&B Rekey Interim Wait
(1) Stop		Start	Start	Start	Start	Start	
(2) Authorized	Op Wait						
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait		
(4) Auth Comp			Op Wait			Rekey Wait	
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait	
(6) Timeout		Op Wait			Rekey Wait		
(7) TEK Refresh Timeout				Rekey Wait			Rekey wait
(8) Key Reply		Operational			Operational		
(9) Key Reject		Start			Start		
(10) GKEK Updated				M&B Rekey Interim Wait			
(11) TEK Updated							Operational